Symantec Mail Security™ for Domino™ Implementation Guide

symantec™

Symantec Mail Security™ for Domino™ Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 4.1
PN: 10332110

Copyright Notice

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Bloodhound, LiveUpdate, Probe Network, Symantec AntiVirus, Symantec Brightmail Logistics and Operations Center (BLOC), Symantec Enterprise Security Architecture (SESA), Symantec Mail Security, and Symantec Security Response are trademarks of Symantec Corporation.
Java, and all Java-based trademarks, Sun, Sun Microsystems, the Sun logo, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. Microsoft, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and other countries. IBM, the IBM logo, Lotus, Domino, and Notes are registered trademarks of IBM Corporation in the United States, other countries, or both. Intel and Pentium are registered trademarks of Intel Corporation. Adobe, Acrobat, and Reader are registered trademarks of Adobe Systems Incorporated in the United States and other countries.
THIS PRODUCT IS NOT ENDORSED OR SPONSORED BY ADOBE SYSTEMS INCORPORATED, PUBLISHERS OF ADOBE ACROBAT.
Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Symantec Corporation Software License Agreement Symantec Mail Security for Domino

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; antispam software utilize updated antispam rules; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. **IN NO CASE SHALL SYMANTEC’S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE.** The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec’s computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State’s Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is Symantec Mail Security for a corresponding third party product or platform, You may only use that Software for the corresponding product or platform. You may only use the Software for the number of users set forth in the License Module.

B. If the Software You have licensed is Symantec Premium AntiSpam, the following terms and conditions apply:

You may use the Software in the quantity licensed to You by Symantec under a License Module until the end date indicated on the License Module ("the End Date"), solely on computing devices owned by you, to filter incoming email sent to Your End Users on Your Email Service;

You must have a license for each End User for whom you use the Software to filter email. "End User" means an employee, contractor or other agent authorized by You as a user of an email mailbox account or an email address hosted by Your Email Service. "Email Service" means Your email services provided to End Users for the purposes of conducting Your internal business and which are enabled via Your mail transfer agent;

You may copy the Software onto Your computing devices as necessary to exercise the rights granted in Section B.1, above; and

You may not use the Software after the End Date.

C. If the Software You have licensed is Symantec Premium AntiSpam, the following additional terms apply to Jikes, a third party technology associated with the Software:

Licensee is entitled to a copy of the source code for Jikes from http://www-124.ibm.com/developerworks/downloads/detail.php?group_id=10&what=rele&id=501. The use of Jikes is governed by the IBM Public License, the full text of which can be found at http://www-124.ibm.com/developerworks/opensource/license10.html (the "IBM License").

OTHER THAN AS PROVIDED IN THIS AGREEMENT, THE CONTRIBUTORS (AS DEFINED IN THE IBM LICENSE) MAKE NO REPRESENATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, WARRANTIES OF TILTE AND NON-INFRINGEMENT, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Other than as otherwise provided in this Agreement, in no event will any of the Contributors be liable for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits.

Any provisions in this License Agreement that differ from the IBM License are offered by Symantec alone and not by any other party.

Contents

Chapter 5 Setting global scanning options

Chapter 6 Establishing antivirus protection

Chapter 7 Filtering unwanted content

Chapter 8 Filtering spam

Chapter 9 Scanning for viruses, spam, and content filtering rule violations

Chapter 10 Configuring LiveUpdate

Chapter 11 Using the Symantec Mail Security for Domino Log

Chapter 12 Managing the Quarantine

Appendix A Automatically routing messages to a spam folder

Appendix B Integrating Symantec Mail Security for Domino with SESA

Index

Chapter 1

Introducing Symantec Mail Security for Domino

This chapter includes the following topics:

About Symantec Mail Security for Domino

Symantec Mail Security for Domino is a complete, customizable, and scalable antivirus, antispam, and content filtering solution. Symantec Mail Security for Domino scans Lotus Notes® database document writes and email messages that pass through the Lotus® Domino™ server. It protects your Lotus Domino server from viruses and destructive programs, filters unwanted content, and identifies unsolicited email messages. You can manage one or more Domino servers with Symantec Mail Security for Domino.

Symantec Mail Security for Domino lets you specify the actions to take and notifications and alerts to issue when a threat or violation is detected. The criteria that are used to identify threats and violations are customizable.

Symantec Mail Security for Domino contains a heuristic antispam engine that identifies spam messages. To further enhance spam detection, you can subscribe to the Symantec Premium AntiSpam service. The premium antispam service provides continual, real-time updates to the Symantec Premium AntiSpam filters. The heuristic antispam engine and the premium antispam service use a shared white list to reduce the incidents of false positives.

The content filtering feature lets you filter undesirable content, such as offensive language and confidential information. You can create and save multiple sets of criteria.

The Lotus Domino environment is only one avenue in which a virus can penetrate your site. For complete virus protection, ensure that every computer and workstation at your site is protected by a desktop antivirus solution.

What's new in Symantec Mail Security for Domino

Table 1-1 lists the new product features in Symantec Mail Security for Domino.

Table 1-1 New features

Feature	Description
Symantec Premium AntiSpam service	The Symantec Premium AntiSpam service provides continual, real-time updates to the Symantec Premium AntiSpam filters. The premium antispam service includes the following features: ■ Reputation service: Symantec monitors email sources to determine how much of the email messages that are sent from those sources is legitimate. Email from those sources can then be blocked or allowed based on the reputation value of the source as determined by Symantec. ■ Comprehensive spam filtering: Symantec Probe Network™ is a global network of decoy email addresses that attracts and collects the latest spam. When spam is received, the Symantec Brightmail Logistics and Operations Center (BLOC™) issues filters that isolate similar spam messages. ■ Enhanced URL filtering: Symantec builds its known-spammer list based on the URLs that appear in spam messages that are collected by the Symantec Probe Network. ■ Enhanced MIME filtering: Symantec downloads a list of MIME filters developed by BLOC and treats any message as spam if any MIME attachment in the message matches a Symantec MIME filter. See "Identifying spam using the premium antispam service" on page 157.

Table 1-1 New features

Feature	Description
Foldering agent	The foldering agent is an application that is designed to work with the Symantec Premium AntiSpam service. It lets you automatically route spam and suspected spam messages to a spam folder in each user's mailbox. The foldering agent also lets users submit missed spam and false positives to the Symantec Brightmail Logistics Operations Center. See "Automatically routing messages to a spam folder" on page 231.
Licensing enhancements	You can activate licensing for multiple servers in a server group at the same time. See "Activating your Symantec Mail Security for Domino licenses" on page 61.

Components of Symantec Mail Security for Domino

Table 1-2 lists the product components that work together to protect your Lotus Domino server.

Table 1-2 Product components

Component	Description	File name
Symantec Mail Security for Domino	This is the software that you install to protect your Lotus Domino server from viruses, detect unwanted email messages, and block unwanted content.	SMSDOM\setup.exe
LiveUpdate™ Administration Utility	This is the utility that lets you configure one or more intranet FTP, HTTP, or LAN servers to act as internal LiveUpdate servers. LiveUpdate lets Symantec products download program and virus definition file updates directly from Symantec or from an intranet LiveUpdate server. For more information, see the LiveUpdate Administrator's Guide on the product CD.	ADMTOOLS\LUA\luau.exe

Table 1-2 Product components

Component	Description	File name
Foldering agent installer	This program installs the foldering agent. The foldering agent works with the Symantec Premium AntiSpam service. It lets you automatically route spam and suspected spam messages to a spam folder in each user's mailbox.	ADMTOOLS/Folder_Agent
SESA Agent installer	This program installs the SESA Agent, which handles the communications between Symantec Mail Security for Domino and SESA. SESA is an event management system that uses data collection services for events that Symantec and supported third-party products generate.	ADMTOOLS\SESA_Agent_Installer\sesa_agent_installer.exe
SESA Integration package	The SESA Integration package extends SESA functionality to include Symantec Mail Security for Domino event data.	ADMTOOLS\SESA_SIPI_for_SMSDOM\
Java Runtime Environment (JRE)	Before you install the SESA Agent, you must install the Java Runtime Environment (JRE) version 1.3.1_02 on the server on which you want to install the SESA Agent.	ADMTOOLS\JRE\j2re-1_3_1_02 - win.exe
Adobe® Acrobat® Reader® 6.0	This is the software that makes it possible to read electronic documentation in Portable Document Format (PDF).	DOCS\ar60enu.exe
Symantec Mail Security for Domino Implementation Guide	This is a PDF version of the Implementation Guide, which provides information on installing and configuring this product.	DOCS\SMSDOM\SMSDOM_WinSvr.pdf

Table 1-2 Product components

Component	Description	File name
Symantec Mail Security for Domino ReadMe file	This text file contains compatibility information and known issues about Symantec Mail Security for Domino.	ReadMe.txt

How Symantec Mail Security for Domino works

In a typical configuration, Symantec Mail Security for Domino scans documents that are written to the Lotus Domino server and scans email messages as they pass through the server. Symantec Mail Security for Domino scans first for viruses, then for spam detection, and then for content filtering rules. Symantec Mail Security for Domino logs violations that are detected during the scan. To reserve system resources, you can configure Symantec Mail Security for Domino to stop the scanning process after the first content filtering rule violation is detected.

See "Setting the action options for a content filtering rule" on page 132.

About scan error violations

When Symantec Mail Security for Domino is unable to scan a document because it is an encrypted container file, it exceeds one or more container limits, or it is unscannable for any reason, it considers the document a scan error violation.

By default, Symantec Mail Security for Domino logs the detection of encrypted container files. However, it quarantines all other types of scan error violation documents. You can change how Symantec Mail Security for Domino disposes of these types of scan error violations.

See "Setting basic antivirus options" on page 105.

When scan error violations are logged in the Log, they appear in the All Incidents view and are assigned a severity indicator.

See "Understanding the Log views" on page 197.

Because a scan error violation is unscannable, when you release a scan error violation document from the Quarantine, the document is not rescanned before it is sent to its destination. Documents that contain scan error violations and virus infections are treated as infected documents in the Quarantine and are rescanned when they are released from the Quarantine.

See "About releasing documents from the Quarantine" on page 219.

Scanning processes

Symantec Mail Security for Domino uses several antivirus technologies to scan documents for viruses. It looks for known viruses by comparing segments of your documents to the sample code inside of a virus definition file. The virus definition file contains nonmalicious bits of code, or virus definitions, for thousands of viruses. Symantec Mail Security for Domino uses Bloodhound™ technology, which provides heuristic detection of new or unknown viruses; NAVEX™, which provides protection from new classes of viruses automatically through LiveUpdate; and Striker, which detects polymorphic viruses.

When Symantec Mail Security for Domino finds a match, the file is considered infected, and the document is disposed (repaired, deleted, quarantined, or logged and delivered) according to the configuration settings. When Symantec Mail Security for Domino receives an email message with an attachment from an Internet source, it decodes and decompresses the attachment and then scans it.

After scanning for viruses, Symantec Mail Security for Domino checks the domain addresses of incoming email messages against a white list, if the white list feature is enabled. Messages sent from white-listed domains automatically bypass the antispam engine and are scanned for content filtering rule violations. All other messages are scanned by the standard antispam engine or the premium antispam service scan engine and are scored based on their probability of being spam.

When antivirus and antispam scanning are complete, documents are then scanned for content filtering rule violations, if content filtering rules processing is enabled. Symantec Mail Security for Domino uses Dynamic Document Review (DDR) technology to analyze the content. Documents are scored against thresholds that are established through content filtering rules, match lists, and word categories. Documents that contain violations are disposed of according to the content filtering configuration settings.

About Symantec Mail Security for Domino databases

Table 1-3 lists the databases that comprise Symantec Mail Security for Domino.

Table 1-3 Symantec Mail Security for Domino databases

Database	Description
Symantec Mail Security for Domino Settings database (sav.nsf)	The Settings database contains the antivirus, antispam, content filtering, and logging configurations in addition to LiveUpdate and licensing information for your Lotus Domino servers. The icon for this database is identified as SMSDOM Settings 4.1 on the Lotus Notes client.
Symantec Mail Security for Domino Log database (savlog.nsf)	The Log database contains server messages, product information, violation incidents, and log reports. The icon for this database is identified as SMSDOM Log 4.1 on the Lotus Notes client.
Symantec Mail Security for Domino Quarantine database (savquar.nsf)	The Quarantine database contains quarantined and backup documents. You can view detailed information about a quarantined or backup document, and you can release a document to its destination. Infected documents are only released when the infected attachment is removed. Documents that are quarantined are stored in the Quarantine until you delete them or until they are purged. The icon for this database is identified as SMSDOM Quarantine 4.1 on the Lotus Notes client.
Symantec Mail Security for Domino Help database (savhelp.nsf)	The Help database contains information about the product and the online Help for Symantec Mail Security for Domino. The icon for this database is identified as SMSDOM Help 4.1 on the Lotus Notes client.
Symantec Mail Security for Domino Definitions database (savdefs.nsf)	The Definitions database contains updated virus definitions. Create this database only if you plan to replicate virus definitions across multiple Domino servers. See "To create a replica Definitions database" on page 78. The icon for this database is identified as SMSDOM Definitions 4.1 on the Lotus Notes client.

About zero maintenance management

Symantec Mail Security for Domino is self-monitoring, which means that it has a heartbeat function that monitors scan threads to ensure that they are working. When problems occur, Symantec Mail Security for Domino posts the events to the Symantec Mail Security for Domino Log.

You can also configure Symantec Mail Security for Domino to post events to Symantec Enterprise Security Architecture (SESA). SESA is an event management system that uses data collection services for events that Symantec and supported third-party products generate.

Symantec Mail Security for Domino sends a subset of security and application events to SESA. The events that Symantec Mail Security for Domino generates include failed virus definitions updates, scans that fail to complete within their configured intervals, servers that are no longer detecting viruses, virus incidents and other violations, and cases in which the number of scan threads that are running falls below two.

See “Integrating Symantec Mail Security for Domino with SESA” on page 237.

For more information about SESA, see the *Symantec Enterprise Security Architecture Installation Guide* and the *Symantec Enterprise Security Architecture Administrator’s Guide*.

Integrating with other Symantec products

Symantec Mail Security for Domino detects the operation of several Symantec products and prevents virus detection conflicts when multiple products are on the same computer. To help prevent virus detection conflicts, Symantec Mail Security for Domino detects whether either of the following products are running:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security

Virus definition files can be shared when any of these Symantec products run on the same computer. When LiveUpdate is performed from one of these programs, it automatically updates the virus definition files that are used by all of the installed Symantec products.

See “About shared virus definition files” on page 182.

Note: If you intend to replicate virus definitions using the Symantec Mail Security for Domino Definitions database (savdefs.nsf), you must run LiveUpdate from Symantec Mail Security for Domino.

See “About replicating Symantec Mail Security for Domino databases” on page 74.

When other Symantec antivirus products are installed on the same computer as Symantec Mail Security for Domino, you must log on to the other products before you log on to Symantec Mail Security for Domino. You might also need to modify some scanning configurations for some of the products.

By default, Symantec Mail Security for Domino uses the Windows TEMP directory when it processes scans, but you can change this directory.

See "Setting basic antivirus options" on page 105.

What you can do with Symantec Mail Security for Domino

Symantec Mail Security for Domino provides the following features to protect and enhance your Lotus Domino server:

- Protect against computer viruses
- Identify unwanted email messages
- Filter undesirable message content
- Manage virus outbreaks
- Isolate infected attachments
- Keep virus protection definitions up-to-date
- Analyze data
- Send notifications when a threat or violation is detected
- Manage single and multiple Lotus Domino servers

Protect against computer viruses

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. After a virus is identified, information about the virus (a virus signature) is stored in a virus definition file. This file contains the necessary information to detect and eliminate the virus. When Symantec Mail Security for Domino scans for viruses, it searches for these virus signatures.

Symantec Mail Security for Domino also uses Symantec Bloodhound heuristics technology to scan for viruses for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors, such as self-replication, to target potentially infected documents.

Symantec Mail Security for Domino scans document writes and email messages that are sent to mailboxes on Lotus Domino servers, including files in compressed and encoded formats, such as Zip. It also decomposes and scans file attachments for viruses.

You can configure Symantec Mail Security for Domino to scan the Domino server on a regular schedule, or you can manually start a scan. The auto-protect feature detects viruses in real-time as email messages are routed through the Lotus Domino server or as documents are written to the server.

Note: To perform any scanning operation, you must have a valid product license. See “About licensing” on page 61.

You can configure Symantec Mail Security for Domino to do any of the following when it detects a virus:

- Log the violation only (does nothing with the infected document)
- Delete the infected document
- Repair the infected document to eliminate viruses automatically on detection
- Quarantine infected documents for administrator review

See “Establishing antivirus protection” on page 101.

Identify unwanted email messages

Spam is unsolicited bulk email, most often advertising messages for a product or service. It wastes productivity time and network bandwidth.

Symantec Mail Security for Domino provides a heuristic antispam detection engine to identify unwanted email messages. You can select the sensitivity level of the antispam engine, prepend the email message subject line with customized text to alert the message recipient that the message is identified as spam, and add a new header field.

See “Configuring standard antispam settings” on page 152.

The Symantec Premium AntiSpam subscription service further enhances spam message detection. The Symantec Premium AntiSpam service uses the latest technologies and strategies to filter and classify email as it enters your site.

See “Identifying spam using the premium antispam service” on page 157.

The white list feature is shared by the standard antispam engine and the premium antispam service. The white list lets you specify domains that are permitted to bypass the antispam scan, thereby reducing the incidents of false positives.

See “Managing a white list” on page 149.

Filter undesirable message content

To enhance protection, Symantec Mail Security for Domino blocks email messages and documents based on content. Symantec Mail Security searches the subject lines or contents of email messages and their attachments for offensive language, confidential information, and content with potential legal consequences.

To scan for unwanted content, you create content filtering rules. When the content of a document or some attribute of an attached file violates a rule, Symantec Mail Security for Domino disposes of the email message according to the settings that you supplied for that rule.

You can set up as many content filtering rules as needed. Each rule specifies the condition that triggers a content filtering rule violation.

See “Filtering unwanted content” on page 113.

Manage virus outbreaks

A virus outbreak occurs when the number of virus detections over a period of time exceeds a specified limit. This outbreak potentially could be the result of a mass-mailer worm or virus.

A mass-mailer worm or virus can infiltrate a computer by exploiting security vulnerabilities and spread by sending copies of itself by email through the Internet or a network. For example, a single mass-mailer worm can infect one computer in an organization and then spread by sending copies of itself through email to everyone in the company’s global address book.

Symantec Mail Security for Domino helps you manage virus outbreaks quickly and effectively by setting outbreak rules and sending alert notifications by email when an outbreak is detected.

When your Domino server is attacked by a mass-mailer worm or virus, the mass-mailer cleanup feature automatically deletes mass-mailer infected messages and their attachments.

See “Managing outbreak detection” on page 110.

Isolate infected attachments

Symantec Mail Security for Domino includes a Quarantine that stores documents or email messages that trigger violations during a scan.

Documents and email messages are placed in the Quarantine under the following circumstances:

- Content filtering is configured to quarantine or copy documents when a content filtering rule violation occurs in a document write, email message, or attachment (as specified by the content filtering rule).
- Any of the auto-protect, scan now, or scheduled scans are configured to quarantine documents after a virus is detected.
- Any of the auto-protect, scan now, or scheduled scans are configured to repair infected attachments, but quarantine any documents that have attachments that cannot be repaired.
- Antivirus scanning is configured to quarantine any documents that contain scan error violations.

You have several options for disposing of a document in the Quarantine, such as saving the document to another location or releasing the document.

See “Managing the Quarantine” on page 213.

Keep virus protection definitions up-to-date

Symantec Mail Security for Domino relies on up-to-date information to detect and eliminate viruses. One of the most common reasons computers are vulnerable to virus attacks is that virus definition files are not updated regularly. Symantec regularly supplies updated virus definition files.

Using LiveUpdate, Symantec Mail Security for Domino connects to a Symantec server over the Internet and automatically determines if virus definitions need to be updated. If they do, the virus definition files are downloaded to the proper location and installed.

See “Configuring LiveUpdate” on page 181.

Note: To receive new virus definitions through LiveUpdate, you must have a valid content license.

See “Activating your Symantec Mail Security for Domino licenses” on page 61.

Analyze data

Symantec Mail Security for Domino gathers and stores the following information in the Log database:

- Server messages: Server-related events
- Product information: Product version, servers on which the product is installed, and virus definitions versions
- Scan reports: Summaries of scheduled and manual scans
- Incidents: Virus, scan errors, spam, and content filtering rule violations
- Statistics: Predefined statistical reports of Log data
- Reporting: Custom reports or queries that you create

See “Using the Symantec Mail Security for Domino Log” on page 195.

Send notifications when a threat or violation is detected

Symantec Mail Security for Domino provides several options for notifying document authors, document recipients, and administrators of threats and violations.

You define the conditions in which to send an alert and determine how to dispense with the document that contains the violation. You can also customize the alert message text for each alert condition that you define.

See “Configuring alerts” on page 90.

Manage single and multiple Lotus Domino servers

Symantec Mail Security for Domino can provide protection for one or more Lotus Domino servers. You can simplify the creation and management of Domino databases across multiple Lotus Domino servers. You choose a single server on which to manage Symantec Mail Security for Domino and receive updated virus definitions. You use Lotus Domino replication technology to synchronize the Symantec Mail Security for Domino databases on the managed server with other servers. You can also use the replication process to send reports on statistics and incidents for all of the servers to the managed server.

For more information about database replication, see your Lotus Domino documentation.

See “Managing multiple servers” on page 74.

See “Updating virus protection” on page 185.

You can also set up server groups to simplify management of multiple Lotus Domino servers. Server groups let you group servers that have a common purpose and, therefore, require the same protection. By grouping servers, you only have to apply a common set of protection settings once, rather than repeatedly to each server.

See “Creating a server group” on page 80.

Where to get more information about Symantec Mail Security for Domino

Symantec Mail Security for Domino provides an extensive system of Help topics that you can access through the Help table of contents, troubleshooting topics, and index. Context-sensitive Help is available on each tab. When you use the Lotus Notes client to view the Symantec Mail Security for Domino databases, you can also access context-sensitive Help for group of options on that tab.

If you are connected to the Internet, you can visit the Symantec Web site for more information about your product. The following online resources are available to you:

www.symantec.com/techsupp/ent/enterprise.html	Provides access to the technical support Knowledge Base, newsgroups, contact information, downloads, and mailing list subscriptions
www.symantec.com/licensing/els/help/en/help.html	Provides information about registration, frequently asked questions, how to respond to error messages, and how to contact Symantec License Administration
securityresponse.symantec.com	Provides access to the Virus Encyclopedia, which contains information about all known viruses; information about virus hoaxes; and access to white papers about virus threats

Installing Symantec Mail Security for Domino

This chapter includes the following topics:

Before you install

Before you install Symantec Mail Security for Domino, become familiar with where the setup program installs the Symantec Mail Security for Domino software. You should also ensure that your environment meets the system requirements.

See “System requirements” on page 31.

The Symantec Mail Security for Domino setup program reads the Windows registry to locate the Lotus Domino server and default data directories. In addition to Symantec Mail Security for Domino registry keys, the following directories are created by default (as needed):

[Domino binary directory]	Symantec Mail Security for Domino engine.
[Domino data directory]\SAV	Symantec Mail Security for Domino databases (sav.nsf, savlog.nsf, savquar.nsf, and savhelp.nsf), ReadMe text file, and a PDF version of the *Symantec Mail Security for Domino Implementation Guide*. If you are going to replicate virus definitions to other Domino servers that are running Symantec Mail Security for Domino, the Definitions database (savdefs.nsf) is created here. See “Updating virus protection with LiveUpdate” on page 185.
[Domino data directory]\SAV\CF	Content filtering rules.
\Program Files\Common Files\Symantec Shared\VirusDefs	Virus definition files (used for all Symantec products).
\Program Files\Symantec\SMSDOM	Premium antispam and runtime data files.
\Program Files\Common Files\Symantec Shared\Licenses	Symantec license files. After you install a license for any Symantec product, the license file is placed in this folder.
\Program Files\Symantec\LiveUpdate	Technology to download virus definition files and program updates (used for all Symantec products).

System requirements

You must have administrator-level privileges to Windows and the Lotus Domino server to install Symantec Mail Security for Domino. Your environment must also meet the following minimum requirements:

Operating system	■ Windows 2000 Server SP3 ■ Windows 2000 Advanced Server SP3 ■ Windows Server 2003 ■ Windows 2003 Enterprise Edition (32-bit only)
Lotus Domino	■ Domino Server 6.5, 6.5.1, 6.5.2, 6.5.3 ■ Domino Server 6.0.2 CF1, 6.0.2 CF2, 6.0.3 ■ Domino Server 5.0.11, 5.0.12, 5.0.13
Lotus Notes	■ Lotus Notes Client 5.0.x, 6.0.x, 6.5.x
Processor	1 GHz Pentium or higher
Memory	256 MB minimum; 512 MB recommended Performance depends on server load.
Disk space to install	100 MB
Available disk space for processing	300 MB minimum The location for temporary files is an option that you can change after installation. See “Setting basic antivirus options” on page 105.
Hardware	CD-ROM drive
Internet browser (for use as a Web access client)	Internet Explorer 6.0 SP1

The premium antispam service has additional system requirements.

See “Installing the product with the premium antispam service” on page 34.

See “Upgrading the product with the premium antispam service” on page 39.

Installing Symantec Mail Security for Domino

Symantec Mail Security for Domino installs with default (but customizable) settings that reduce routine maintenance. For example, an outbreak management threshold limit is set during installation so that administrators receive notification when too many suspicious documents are detected on the Lotus Domino server over a set interval. These default settings can be changed.

If you are installing over a previous version or reinstalling the product, use the procedures for upgrading Symantec Mail Security for Domino.

See "Upgrading Symantec Mail Security for Domino" on page 35.

If you have multiple Lotus Domino partitions on the same server, the installation program detects each one and lets you specify the partitions on which to install Symantec Mail Security for Domino.

To facilitate enterprise-wide management of Symantec Mail Security for Domino, you can replicate the Symantec Mail Security for Domino databases to other servers that run Symantec Mail Security for Domino. With replication, you can configure Symantec Mail Security for Domino settings from a single server, report virus incidents and statistics for all servers, and use a single virus definitions update to maintain current protection for all servers.

See "About administering Symantec Mail Security for Domino on multiple servers" on page 73.

After the installation process is complete and you start the Lotus Domino server, the Symantec Mail Security for Domino databases are created from templates and are placed in the SAV subdirectory of your default Data directory.

When you are finished installing Symantec Mail Security for Domino, you should perform the post-installation tasks.

See "Post-installation tasks" on page 40.

Installing the product without the premium antispam service

Before you install Symantec Mail Security for Domino, you must stop any Lotus Domino partitions that are running on the computer (and the Lotus Notes client or Web client if either is on the same computer as the server partitions).

Additional preparation and configuration is required to use the Symantec Premium AntiSpam service.

See "Installing the product with the premium antispam service" on page 34.

To install the product without the premium antispam service

1. Insert the Symantec Mail Security for Domino installation CD into your CD-ROM drive.

   The installation program launches automatically. If it does not, you should run cdstart.exe from the installation CD.

2. On the Symantec Mail Security for Domino installation screen, click **Install Symantec Mail Security for Domino** to begin the installation process.

3. Read the on-screen instructions, and then click **Next** to continue.

4. Indicate that you accept the terms of the Symantec software license agreement, and then click **Next**.

   You must accept the terms of the license agreement for the installation to continue.

5. In the Choose Destination Location panel, do one of the following:

   - To install the product in the default location, click **Next**.
   - To install the product in a different location, click **Browse**, select the location of the installation folder, click **OK**, and then click **Next**.

     The installation directory must end with \SMSDOM

6. To continue the installation process without installing the premium antispam service, in the Premium AntiSpam panel, under Do you intend to utilize the Premium AntiSpam service, click **No**, and then click **Next**.

7. If you have multiple Lotus Domino partitions on the same server, in the Select Servers dialog box, select the partitions on which to install Symantec Mail Security for Domino.

8. To optionally select additional partitions, click **Add Additional Partitions**, and then in the Select data directory dialog box, type the partition path or browse directories to select a path, and then click **OK**.

9. Read through the remaining panels, and then click **Next** until you reach the Complete Setup panel.

10. In the Complete Setup panel, click **Finish**.

11. If prompted, restart your computer.

12. Start the Lotus Domino server, if necessary.

Installing the product with the premium antispam service

Before you install Symantec Mail Security for Domino with the premium antispam service, do the following:

- Read "Before you install and enable the premium antispam service" on page 153.
- Ensure that Microsoft Internet Information Services (IIS) is installed and that the SMTP service and IIS Administration are enabled.
- Ensure that you have applied the most recent security updates from Microsoft for Microsoft IIS and Microsoft SMTP service.
- Uninstall Brightmail AntiSpam™ if it is installed on your server.
- Stop any Lotus Domino partitions that are running on the computer (and the Lotus Notes client or Web client if either is on the same computer as the server partitions).

See "Installing the product without the premium antispam service" on page 32.

To install the product with the premium antispam service

1. Insert the Symantec Mail Security for Domino installation CD into your CD-ROM drive.
   The installation program launches automatically. If it does not, you should run cdstart.exe from the installation CD.
2. On the Symantec Mail Security for Domino installation screen, click **Install Symantec Mail Security for Domino** to begin the installation process.
3. Read the on-screen instructions, and then click **Next** to continue.
4. Indicate that you accept the terms of the Symantec software license agreement, and then click **Next**.
   You must accept the terms of the license agreement for the installation to continue.
5. In the Choose Destination Location panel, do one of the following:
   - To install the product in the default location, click **Next**.
   - To install the product in a different location, click **Browse**, select the location of the installation folder, click **OK**, and then click **Next**.
     The installation directory must end with \SMSDOM
6. To install the premium antispam service, in the Premium AntiSpam panel, under Do you intend to utilize the Premium AntiSpam service, click **Yes**, and then click **Next**.
7. To let the setup program disable unnecessary IIS services, in the Harden IIS panel, click **Yes**, and then click **Next**.

8 If you have multiple Lotus Domino partitions on the same server, in the Select Servers dialog box, select the partitions on which to install Symantec Mail Security for Domino.

9 To optionally select additional partitions, click **Add Additional Partitions**, and then in the Select data directory dialog box, type the partition path or browse directories to select a path, and then click **OK**.

10 Read through the remaining panels, and then click **Next** until you reach the Complete Setup panel.

11 In the Complete Setup panel, click **Finish**.

12 If prompted, restart your computer.

13 Start the Lotus Domino server, if necessary.

Upgrading Symantec Mail Security for Domino

Symantec Mail Security for Domino supports upgrades from Symantec AntiVirus™/Filtering for Domino™ version 3.1 and Symantec Mail Security for Domino version 4.0.x.

If you have multiple Lotus Domino partitions on the same server, the installation program detects each one and lets you specify the partitions on which to install Symantec Mail Security for Domino.

To facilitate enterprise-wide management of Symantec Mail Security for Domino, you can replicate the Symantec Mail Security for Domino databases to other servers that run Symantec Mail Security for Domino. With replication, you can configure Symantec Mail Security for Domino settings from a single server, report virus incidents and statistics for all servers, and use a single virus definitions update to maintain current protection for all servers.

See “About administering Symantec Mail Security for Domino on multiple servers” on page 73.

When you upgrade to Symantec Mail Security for Domino, you can upgrade your previous databases.

Table 2-1 describes the information that you should consider before you upgrade your databases.

Table 2-1 Database upgrade considerations

Issue	Additional information
The editable text areas are copied into Symantec Mail Security for Domino exactly as they appear in Symantec AntiVirus/Filtering for Domino 3.1.	For example, if your native MIME header text was configured to read, “The body of this message was deleted by Symantec AntiVirus/ Filtering because it was infected,” it will read exactly the same after you upgrade to Symantec Mail Security for Domino. The former product name is not automatically modified to read Symantec Mail Security for Domino.
Symantec AntiVirus/Filtering for Domino 3.1 had separate backup options for repairing and deleting attachments. Symantec Mail Security for Domino combines these options.	If both options in Symantec AntiVirus/Filtering for Domino 3.1 are the same (that is, both are Yes or both are No), when you upgrade to Symantec Mail Security for Domino, that setting is the default setting. If both options in Symantec AntiVirus/Filtering for Domino 3.1 are different (that is, one is No and the other is Yes), the default setting in Symantec Mail Security for Domino is Yes. See “Creating backup documents” on page 86.
If you enabled any of the agents in a previous version, you must enable them again after you upgrade to Symantec Mail Security for Domino.	For a user to enable, disable, or modify a purge agent, the administrator must grant rights to run unrestricted agents in the Server Document that belongs to the server within the Domino Directory (names.nsf). See “Enabling the Log purge agent” on page 202. See “Purging the Quarantine” on page 229. See “Enabling the Definitions purge agent” on page 192. See “Granting rights to run unrestricted agents” on page 47.

Table 2-1 Database upgrade considerations

Issue	Additional information
If you enabled the scheduled reports agent in a previous version, you must enable it again after you upgrade to Symantec Mail Security for Domino.	For a user to enable, disable, or modify the scheduled reports agent, the administrator must grant rights to run unrestricted agents in the Server Document that belongs to the server within the Domino Directory (names.nsf). See "Enabling the scheduled reports agent" on page 211. See "Granting rights to run unrestricted agents" on page 47.

When the Lotus Domino server is started, the databases that you choose to keep during the installation process will be upgraded. You can verify that the previous databases were properly upgraded by viewing the server console messages.

Any new databases are created from templates and are placed in the SAV subdirectory of your default Data directory.

When you finish upgrading Symantec Mail Security for Domino, you should perform the post-installation tasks.

See "Post-installation tasks" on page 40.

Upgrading the product without the premium antispam service

Before you upgrade Symantec Mail Security for Domino, you must stop the Lotus Domino partitions that are running on the computer (and the Lotus Notes client or Web client if either is on the same computer as the server partitions).

Additional preparation and configuration is required to use the Symantec Premium AntiSpam service.

See "Upgrading the product with the premium antispam service" on page 39.

To upgrade the product without the premium antispam service

1. Insert the Symantec Mail Security for Domino installation CD into the CD-ROM drive.
   The installation program launches automatically. If it does not, you should run cdstart.exe from the installation CD.
2. On the Symantec Mail Security for Domino installation screen, click **Install Symantec Mail Security for Domino** to begin the installation process.
3. Read the on-screen instructions, and then click **Next** to continue.

4. Indicate that you agree with the terms of the Symantec software license agreement, and then click **Next**.

   You must accept the terms of the license agreement for the installation to continue.

5. In the Choose Destination Location panel, do one of the following:

   - To install the product in the default location, click **Next**.
   - To install the product in a different location, click **Browse**, select the location of the installation folder, click **OK**, and then click **Next**.

     The installation directory must end with \SMSDOM

   This panel does not appear if you have previously installed the premium antispam service.

6. To continue the installation process without installing the premium antispam service, in the Premium AntiSpam panel, under Do you intend to utilize the Premium AntiSpam service, click **No**, and then click **Next**.

7. If you have multiple Lotus Domino partitions on the same server, in the Select Servers dialog box, select the partitioned drives on which to install Symantec Mail Security for Domino.

8. To optionally select additional partitions, click **Add Additional Partitions**, and then in the Select data directory dialog box, type the partition path or browse directories to select a path, and then click **OK**.

9. During installation, when you are prompted whether to keep settings from the previous versions of the databases, select the databases that you want to keep.

   The option to keep the Definitions database settings is available only when Symantec Mail Security for Domino detects that a Definitions database exists on the server on which you are installing the product.

   All available databases are checked by default.

10. Read through the remaining panels, and then click **Next** until you reach the Complete Setup panel.

11. In the Complete Setup panel, click **Finish**.

12. If prompted, restart your computer.

13. Start the Lotus Domino server, if necessary.

Upgrading the product with the premium antispam service

Before you upgrade Symantec Mail Security for Domino with the premium antispam service, do the following:

- Read "Before you install and enable the premium antispam service" on page 153.
- Ensure that Microsoft Internet Information Services (IIS) is installed and that the SMTP service and IIS Administration are enabled.
- Ensure that you have applied the most recent security updates from Microsoft for Microsoft IIS and Microsoft SMTP service.
- Uninstall Brightmail AntiSpam if it is installed on your server.
- Stop any Lotus Domino partitions that are running on the computer (and the Lotus Notes client or Web client if either is on the same computer as the server partitions).

If you are installing over a previous version, you must disable the premium antispam service before you reinstall the product.

See "Enabling and disabling the premium antispam service" on page 159.

See "Upgrading the product without the premium antispam service" on page 37.

To upgrade the product to use the premium antispam service

1. Insert the Symantec Mail Security for Domino installation CD into the CD-ROM drive.
   The installation program launches automatically. If it does not, you should run cdstart.exe from the installation CD.
2. In the Symantec Mail Security for Domino installation screen, click **Install Symantec Mail Security for Domino** to begin the installation process.
3. Read the on-screen instructions, and then click **Next** to continue.
   Indicate that you agree with the terms of the Symantec software license agreement, and then click **Next**.
   You must accept the terms of the license agreement for the installation to continue.
4. In the Choose Destination Location panel, do one of the following:
   - To install the product in the default location, click **Next**.
   - To install the product in a different location, click **Browse**, select the location of the installation folder, click **OK**, and then click **Next**.
     The installation directory must end with \SMSDOM

   This panel does not appear if you have previously installed the premium antispam service.

5 To install the premium antispam service, in the Premium AntiSpam panel, under Do you intend to utilize the Premium AntiSpam service, click **Yes**, and then click **Next**.

6 To let the setup program disable unnecessary IIS services, in the Harden IIS panel, click **Yes**, and then click **Next**.

7 If you have multiple Lotus Domino partitions on the same server, in the Select Servers dialog box, select the partitioned drives on which to install Symantec Mail Security for Domino.

8 To optionally select additional partitions, click **Add Additional Partitions**, and then in the Select data directory dialog box, type the partition path or browse directories to select a path, and then click **OK**.

9 During installation, when you are prompted whether to keep settings from the previous versions of the databases, select the databases that you want to keep.
The option to keep the Definitions database settings is available only when Symantec Mail Security for Domino detects that a Definitions database exists on the server on which you are installing the product.
All available databases are checked by default.

10 Read through the remaining panels, and then click **Next** until you reach the Complete Setup panel.

11 In the Complete Setup panel, click **Finish**.

12 If prompted, restart your computer.

13 Start the Lotus Domino server, if necessary.

Post-installation tasks

Table 2-2 describes the tasks that you should perform after you install or upgrade to Symantec Mail Security for Domino.

Table 2-2 Post-installation tasks

Task	Description
Read the ReadMe file.	This text file contains compatibility information and known issues about Symantec Mail Security for Domino. The ReadMe.txt file is located in the [Domino data directory]\SAV directory and on the installation CD.

Table 2-2 Post-installation tasks

Task	Description
Sign the Symantec Mail Security for Domino databases.	Before you open the databases for the first time, you can sign the Symantec Mail Security for Domino databases with a trusted Notes ID file. See "Signing Symantec Mail Security for Domino databases" on page 42.
Set access control.	The access control settings establish who can access the Symantec Mail Security for Domino databases. See "Setting access control for Symantec Mail Security for Domino databases" on page 43.
Access the Symantec Mail Security for Domino databases.	Symantec Mail Security for Domino can be accessed from the Lotus Notes client or a Web browser client. See "Accessing Symantec Mail Security for Domino" on page 44.
Grant rights to run unrestricted agents.	This option gives a user the rights to enable, disable, or modify unrestricted agents. See "Granting rights to run unrestricted agents" on page 47.
Modify the number of processing threads.	Symantec Mail Security for Domino automatically configures the optimum number of scanning threads, but you can modify this number, if necessary. See "Modifying the number of processing threads" on page 48.
Activate licenses.	You must purchase and activate a content license and product license to receive updated virus definition files and to operate any of the Symantec Mail Security for Domino scanning functions. You must also purchase and activate a Symantec Premium AntiSpam license to enable the premium antispam service. See "About licensing" on page 61.
Maximize product performance.	Configure Symantec Mail Security for Domino to maximize performance. See "Optimizing Symantec Mail Security for Domino performance" on page 49.
Enable the premium antispam service, if applicable.	If you disabled the premium antispam service (which is required to install the product over a previous version), you must re-enable it. See "Enabling and disabling the premium antispam service" on page 159.

Signing Symantec Mail Security for Domino databases

The first time that you start the Lotus Domino server after installation, Symantec Mail Security for Domino attempts to digitally sign portions of the Settings, Log, and Quarantine databases. This is required for minimal operation of the software.

To minimize the impact on performance, Symantec Mail Security for Domino does not attempt to sign every design element. The first time that you attempt to open an unsigned database, you are prompted whether to trust unsigned code.

Trusting unsigned code is a security risk because it violates the integrity of the workstation. Before you open the databases for the first time, sign the databases with a trusted Notes ID file, using the Domino Administrator client. To properly sign the Symantec Mail Security for Domino databases, there are several options that you must configure.

In the Domino Administrator client, in the Sign Database dialog box, ensure that the following settings are configured:

- Under What do you want to sign, select All design documents.
- Uncheck the option Update the existing signatures only (faster).
- In Domino 6.x, repeat the database signing steps, and Under What do you want to sign, select All data documents. Ensure that you use an administrator ID to sign databases.

Configure the ID as follows:

- The ID should sign all design documents (and all data documents if you are using the Domino 6.x Administrator client), not just those with existing signatures.
- It should be a trusted administrator's ID or server ID.
- The ID should have the right to run unrestricted LotusScript/Java agents (Domino 5) or run unrestricted Methods and Operations (Domino 6.x). This is necessary to run all of the database agents.
  See "Granting rights to run unrestricted agents" on page 47.
- The ID used to sign the databases should appear on the workstation's Execution Control List (ECL).

In the Execution Control List of your Notes client, ensure that this trusted Notes ID is listed with the following rights:

- Access to current database
- Access to environment variables
- Access to external code
- Access to external programs
- Ability to read other databases
- Ability to modify other databases
- Ability to export data

For more information on signing databases, see the Domino Administrator documentation.

Setting access control for Symantec Mail Security for Domino databases

To maintain antivirus security in your Lotus Domino environment, restrict access to the Symantec Mail Security for Domino databases to administrators by setting the Access Control List (ACL) for the following databases:

- Symantec Mail Security for Domino Settings (sav.nsf)
- Symantec Mail Security for Domino Log (savlog.nsf)
- Symantec Mail Security for Domino Quarantine (savquar.nsf)
- Symantec Mail Security for Domino Definitions (savdefs.nsf), if used

The Quarantine database requires that you also assign roles to Quarantine database users. These roles restrict access to various Quarantine views and control who can release documents from the Quarantine.

See “Managing quarantined documents” on page 214.

When you set access control for the Quarantine database, you must assign roles to those groups and users who use the Quarantine.

See “Assigning Quarantine roles” on page 216.

To set access control for Symantec Mail Security for Domino databases

1. Log on to the account that you plan to use to administer Symantec Mail Security for Domino.
2. In the Lotus Notes workspace, right-click the **Settings** database, and then click **Database** > **Access Control**.

3. In the Access Control List window, add yourself, a group, or other users as necessary to the Access Control List as Managers with Delete Documents rights.
4. In the Access Control List window, click **Default**.
5. In the Access list, click **No Access**.
6. Click **OK**.
7. Repeat steps 1 - 6 for the rest of the Symantec Mail Security for Domino databases.

Accessing Symantec Mail Security for Domino

Symantec Mail Security for Domino runs as a Domino server task. Every time that you start the Domino server, Symantec Mail Security for Domino protection begins. You access management and configuration tasks through the Lotus Notes client or a Web client.

Accessing Symantec Mail Security for Domino from Lotus Notes

Symantec Mail Security for Domino is fully integrated with the Lotus Notes environment and can be accessed like any other database.

To access Symantec Mail Security for Domino from Lotus Notes

1. In Lotus Notes, on the File menu, click **Database** > **Open**.
2. In the Open Database dialog box, under Server, select the server on which you installed Symantec Mail Security for Domino.
3. Under Database, in the SAV directory, double-click **SMSDOM Settings 4.1** (the Settings database).
4. Drag the SMSDOM Settings database window tab to any Lotus Notes bookmark folder.
5. Follow steps 1 - 4 to place the Help, Log, and Quarantine database shortcuts in your Lotus Notes bookmark folder.

Accessing Symantec Mail Security for Domino remotely from a Web browser

In addition to accessing Symantec Mail Security for Domino from the Lotus Notes client, you can access the Log, Quarantine, Definitions, and Help databases remotely over the Internet using Internet Explorer 6.0 SP1 or later.

When you access Symantec Mail Security for Domino remotely from a Web browser, you will only be able to perform specific tasks or access certain information. Only the tasks that you can perform or information that you can access will appear on the Web browser screen.

The following tasks and data are not available through the Web browser:

Settings database	This database is inaccessible through a Web browser.
Log database	■ Export incidents to Microsoft Excel. ■ Open links in the Server Messages or Incidents views. ■ Open Virus, Spam Detection, or Content Filtering statistics in the Statistics view. ■ Enable the purge agent. ■ Enable the scheduled reports agent. See “About logging” on page 195.
Quarantine database	■ Release infected documents or content filtering rule violation documents from the Quarantine. ■ View the Quarantined Content Filtering Violation report. ■ Enable the purge agent. See “About the Quarantine” on page 213.
Definitions database	■ Set active definitions. ■ Enable the purge agent. See “Managing the Definitions database” on page 190.
Help database	Context-sensitive Help for group options is unavailable through a Web browser.

To access Symantec Mail Security for Domino databases over the Internet, you must load HTTP on the Domino server. You can load HTTP at the command prompt or by modifying the Notes.ini file.

To load HTTP at the command prompt

◆ In the Domino server console, at the command prompt, type the following:

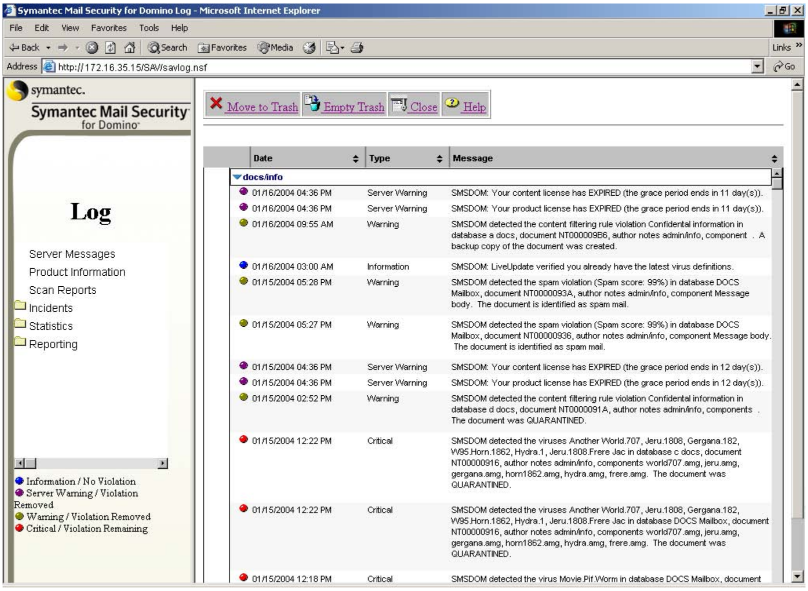
```
LOAD HTTP
```

To load HTTP by modifying the Notes.ini file

1. Stop the Domino server.
2. In the Notes.ini file, add **HTTP** to the entries in the ServerTasks= line.
3. Save and close the file.
4. Start the Domino server.

To access Symantec Mail Security for Domino remotely from a Web browser

1. Open Internet Explorer 6.0 SP1 or later.
2. In the address field of the browser, type the IP address of the Domino server on which Symantec Mail Security for Domino is installed, followed by the path name of the Symantec Mail Security for Domino database that you want to access.
   For example:
   http://172.16.35.15/SAV/savlog.nsf
3. Type your server login user name and password.


Symantec Mail Security for Domino Log - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Address http://172.16.35.15/SAV/savlog.nsf
Go
symantec.
Symantec Mail Security for Domino
Log
Server Messages
Product Information
Scan Reports
Incidents
Statistics
Reporting
Move to Trash
Empty Trash
Close
Help
● Information / No Violation
● Server Warning / Violation Removed
● Warning / Violation Removed
● Critical / Violation Remaining

	Date	Type	Message
docs/info			
●	01/16/2004 04:36 PM	Server Warning	SMSDOM: Your content license has EXPIRED (the grace period ends in 11 day(s)).
●	01/16/2004 04:36 PM	Server Warning	SMSDOM: Your product license has EXPIRED (the grace period ends in 11 day(s)).
●	01/16/2004 09:55 AM	Warning	SMSDOM detected the content filtering rule violation Confidental information in database a docs, document NT000009B6, author notes admin/info, component . A backup copy of the document was created.
●	01/16/2004 03:00 AM	Information	SMSDOM: LiveUpdate verified you already have the latest virus definitions.
●	01/15/2004 05:28 PM	Warning	SMSDOM detected the spam violation (Spam score: 99%) in database DOCS Mailbox, document NT0000093A, author notes admin/info, component Message body. The document is identified as spam mail.
●	01/15/2004 05:27 PM	Warning	SMSDOM detected the spam violation (Spam score: 99%) in database DOCS Mailbox, document NT00000936, author notes admin/info, component Message body. The document is identified as spam mail.
●	01/15/2004 04:36 PM	Server Warning	SMSDOM: Your content license has EXPIRED (the grace period ends in 12 day(s)).
●	01/15/2004 04:36 PM	Server Warning	SMSDOM: Your product license has EXPIRED (the grace period ends in 12 day(s)).
●	01/15/2004 02:52 PM	Warning	SMSDOM detected the content filtering rule violation Confidental information in database d docs, document NT0000091A, author notes admin/info, components . The document was QUARANTINED.
●	01/15/2004 12:22 PM	Critical	SMSDOM detected the viruses Another World.707, Jeru.1808, Gergana.182, W95.Horn.1862, Hydra.1, Jeru.1808.Frere Jac in database c docs, document NT00000916, author notes admin/info, components world707.amg, jeru.amg, gergana.amg, horn1862.amg, hydra.amg, frere.amg. The document was QUARANTINED.
●	01/15/2004 12:22 PM	Critical	SMSDOM detected the viruses Another World.707, Jeru.1808, Gergana.182, W95.Horn.1862, Hydra.1, Jeru.1808.Frere Jac in database DOCS Mailbox, document NT00000916, author notes admin/info, components world707.amg, jeru.amg, gergana.amg, horn1862.amg, hydra.amg, frere.amg. The document was QUARANTINED.
●	01/15/2004 12:18 PM	Critical	SMSDOM detected the virus Movie.Pif.Worm in database DOCS Mailbox, document

Tabs in the Lotus Notes user interface are represented as hyperlinks in the Web client.

Granting rights to run unrestricted agents

Symantec Mail Security for Domino contains agents to help you manage database size and run scheduled queries. You must grant rights to the user who signs the IDs.

See "Signing Symantec Mail Security for Domino databases" on page 42.

The agents are as follows:

- Log purge agent: Purges events from the Log database
  By default, virus incidents are purged after 365 days. Server messages and other incidents are purged every 30 days.
  See "Enabling the Log purge agent" on page 202.
- Quarantine purge agent: Purges items from the Quarantine database
  By default, all items in the Quarantine are purged after 30 days.
  See "Purging the Quarantine" on page 229.
- Definitions purge agent: Purges virus definitions from the Definitions database
  By default, only the five most current virus definitions are saved. The remaining are purged.
  See "Enabling the Definitions purge agent" on page 192.
- Scheduled reports agent: Runs scheduled queries in the Log database
  By default, this agent runs scheduled queries once a day and posts the queries in the Completed Reports view.
  See "Enabling the scheduled reports agent" on page 211.

For a user to enable, disable, or modify an agent, the administrator must grant rights to run unrestricted agents in the Server Document that belongs to the server within the Domino Directory (names.nsf).

To grant rights to run unrestricted agents

1. Open Domino Administrator.
2. On the Configuration tab, in the left pane, double-click **Server**.
3. In the left pane, under Server, click **All Server Documents**.
4. In the right (view) pane, double-click the server on which Symantec Mail Security for Domino runs.
5. On the Action bar, click **Edit server**.

6 On the Security tab, do one of the following:

- If you are running Lotus Domino 6.x, under Programmability Restrictions, in the Run unrestricted methods and operations box, add the users to whom you want to grant rights to enable, disable, or modify agents.
- If you are running Lotus Domino 5.x, under Agent Restrictions, in the Run unrestricted LotusScript/Java agents box, add the users to whom you want to grant rights to enable, disable, or modify agents.

7 On the Action bar, click **Save & Close**.

Modifying the number of processing threads

Symantec Mail Security for Domino automatically configures the optimum number of processing threads. The minimum number of threads is two per processor. The maximum number of threads is four per processor.

The default configuration ensures the best performance for your Lotus Domino server. You should not need to modify the number of processing threads.

Warning: If you are uncertain about how a change to the number of processing threads might affect your Domino server, you should maintain the default settings. Modifying the number of processing threads could result in an adverse affect on server performance.

To modify the number of processing threads

1 Turn off the Domino server.

2 In the Domino program directory, make a backup copy of the Notes.ini file.

3 Open Notes.ini in a text editor.

4 Add the following settings:
SAVMailThreads=(value)
SAVWriteThreads=(value)
where (value) is the newly computed number of threads

5 Save the Notes.ini file.

6 Exit the text editor.

7 Start the Domino server.

Optimizing Symantec Mail Security for Domino performance

The following settings let you manage resource demands:

Scan only specific databases.

You can exclude specific databases or directories from scans that might not be at risk for virus infection or require content filtering.

See “Specifying what to scan” on page 84.

Scan only certain file extensions.

Symantec Mail Security for Domino is configured by default to scan all files regardless of extension. Although this is the most secure setting, it also imposes the heaviest demand on resources. You can specify which file name extensions to scan.

See “Specifying what to scan” on page 84.

Do not scan items from a trusted server.

Symantec Mail Security for Domino lets you increase Lotus Domino email delivery performance by reducing scanning redundancy through the use of trusted servers. A trusted server is typically one that you know to be safe from outside security breaches, by means of a firewall or similar protection device or software, and that is already scanning email traffic for viruses, content filtering rule violations, and spam.

See “Configuring trusted server options” on page 89.

Stop rules processing after the first content violation.

You can configure Symantec Mail Security for Domino to stop the processing of other content filtering rules after the first content filtering rule violation is detected. This option optimizes performance by preventing unnecessary processing of a document.

See “Setting the action options for a content filtering rule” on page 132.

Ignore specific server processes from auto-protect scanning.

Symantec Mail Security for Domino must be configured to bypass specific server processes from auto-protect scanning. Symantec Mail Security for Domino provides a default list of server processes that can be ignored.

See “About auto-protect scanning” on page 168.

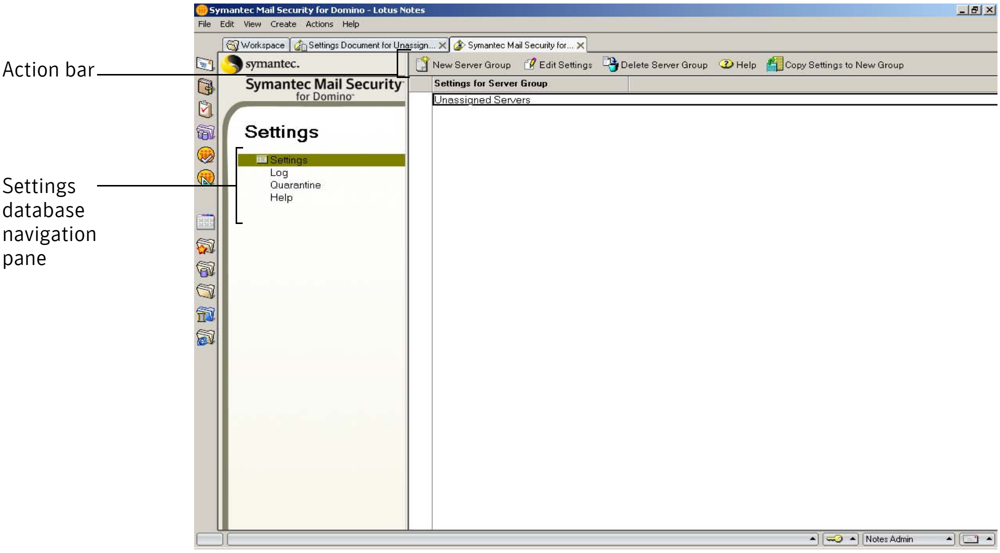
About the Symantec Mail Security for Domino user interface

When you open any of the Symantec Mail Security for Domino databases, you see the database view. When you double-click any item in the right pane, you open a Notes document. The document title appears below the Action bar. A view can easily be distinguished from a document because a view contains a navigation pane on the left.

From the Settings navigation pane, you can open the Log, Quarantine, and Help databases. The ability to open the Symantec Mail Security for Domino databases from the navigation pane is only available in the Settings database.

Figure 2-1 shows the Settings database view.

Figure 2-1 Symantec Mail Security for Domino Settings view


Action bar
Settings database navigation pane
Symantec Mail Security for Domino - Lotus Notes
File Edit View Create Actions Help
Workspace
Settings Document for Unassign...
Symantec Mail Security for...
symantec.
Symantec Mail Security for Domino
Settings
Settings
Log
Quarantine
Help
New Server Group
Edit Settings
Delete Server Group
Help
Copy Settings to New Group
Notes Admin

Settings for Server Group

Unassigned Servers

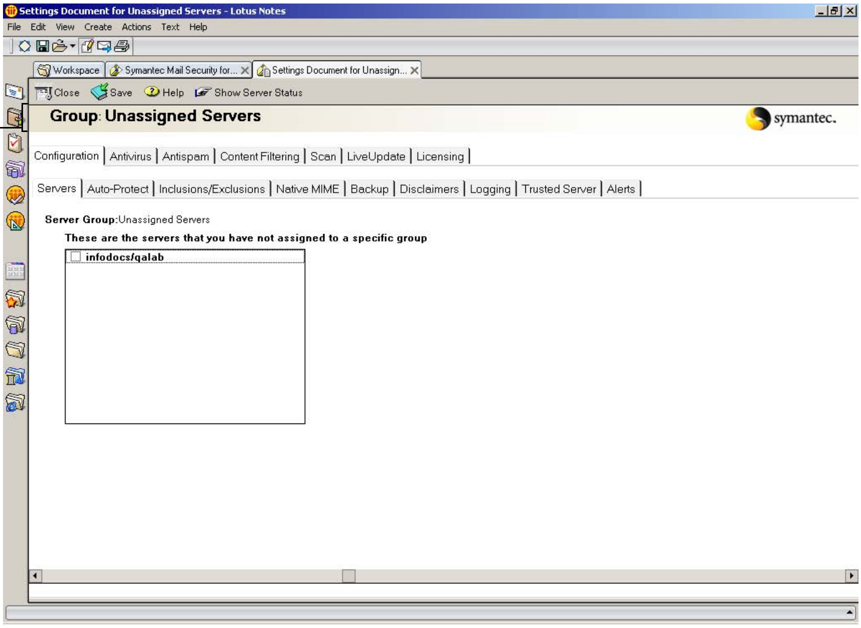
The configuration settings for Symantec Mail Security for Domino are made in the Settings database. In the Settings view, you see an Unassigned Servers server group and any other server groups that you have created. An Unassigned Servers server group always exists and contains any servers that are not assigned to a server group. The Unassigned Servers server group cannot be deleted.

See "Creating a server group" on page 80.

The Group[server group name] document contains the configuration tabs on which you configure all Symantec Mail Security for Domino options.

Figure 2-2 shows the Group document for the Unassigned Server group.

Figure 2-2 Symantec Mail Security for Domino Group document


Settings Document for Unassigned Servers - Lotus Notes
File Edit View Create Actions Text Help
Workspace
Symantec Mail Security for...
Settings Document for Unassign...
Close
Save
Help
Show Server Status
symantec.
Configuration | Antivirus | Antispam | Content Filtering | Scan | LiveUpdate | Licensing
Servers | Auto-Protect | Inclusions/Exclusions | Native MIME | Backup | Disclaimers | Logging | Trusted Server | Alerts

Group: Unassigned Servers

Server Group:Unassigned Servers

These are the servers that you have not assigned to a specific group

☐ infodocs/qalab

Document title

Checking server status

You can check the status of the server on which the Settings database is installed. Checking server status helps you determine if SESA logging is enabled, disabled, or disconnected, or if mass-mailer cleanup, spam detection, content filtering, and outbreak detection are activated.

You can also check the expiration dates for your product, content, and premium antispam licenses.

To check server status

1 In the Settings view, double-click a server group.

2 On the Action bar, click **Show Server Status**.

3 On the Action bar, click **Check Statistics**.
See “Server status errors” on page 52.

4 If necessary, click **Reset Statistics** to restart the status counter and prepare for the next status inquiry.

5 Click **Close** to close the Server Status document.

Troubleshooting status errors

Symantec Mail Security for Domino relies on connections with the server and, particularly, on connections with the NNTASK process to provide server status. If the server is unresponsive or if the connection with NNTASK has failed, then Symantec Mail Security for Domino is unable to provide the current status.

You might receive status error messages in the following situations:

- Checking the server status
  See "Server status errors" on page 52.
- Installing a license file
  See "License installation status errors" on page 53.
- Checking a scan status
  See "Scan status errors" on page 54.
- Checking a LiveUpdate status
  See "LiveUpdate status errors" on page 55.

Server status errors

You can check the status of your Lotus Domino server from the Settings database to ensure that antivirus, content filtering, and spam detections are activated. You can also check the status of your licenses and the date of your most recent virus definitions.

See "Checking server status" on page 51.

When a server status cannot be determined because of an unresponsive server, you receive the following error message:

```
Waiting for response from server. Click "Check Statistics" again.
(When no response occurs after 5 minutes, a communication error with
NNTASK might have occurred. See documentation for more information).
```

When you receive this message, one of the following events might have occurred:

- NNTASK might be under a heavy load and unable to immediately respond to the user's status request.
- NNTASK might not be running on the server.
- The network might be slow.

After you resolve the issue, you should close the Server Status document, and check the server status again.

If Symantec Mail Security for Domino can confirm that the connection with NNTASK has failed, you receive the following error message:

```
Error communicating with NNTASK. Click Close and try again.
```

After you close the Server Status document, you can check the server status again.

License installation status errors

At the end of the license installation process, you receive a License Installation Status document, which lets you verify that your license is properly installed.

See "About license activation" on page 62.

Table 2-3 lists the error messages that you might receive if an error occurs during license installation.

Table 2-3 License installation status errors

Error message	Explanation
Error: Cannot open SMSDOM Settings database. License installation failed.	Occurs when the Settings database cannot be opened. This error might occur because Symantec Mail Security for Domino is not installed or because the Domino server is not running.
Error: Could not issue license install command. License installation failed.	Occurs when the user does not have privileges to create and read documents in the Settings database for that server.

Table 2-3 License installation status errors

Error message	Explanation
Error communicating with NNTASK. Please retry license installation for this server.	Occurs when Symantec Mail Security for Domino confirms that the connection with NNTASK on the server has failed. When you receive this message, one of the following events might have occurred: ■ NNTASK might be under a heavy load and unable to immediately respond to the user's status request. ■ NNTASK might not be running on the server. ■ The network might be slow.

After you resolve the issue, close the License Installation Status document and install the license file again for that server.

Scan status errors

When you perform a scan now (on-demand) scan from the Lotus Notes client, you can check the status of the scan.

See "Configuring scan now settings" on page 171.

When a scan status cannot be determined because of an unresponsive server, you receive the following error message:

```
Waiting for response from server. Click "Check Scan Status" again.
(When no response occurs after 5 minutes, a communication error with
NNTASK might have occurred. See documentation for more information).
```

When you receive this message, one of the following events might have occurred:

- NNTASK might be under a heavy load and unable to immediately respond to the user's status request.
- NNTASK might not be running on the server.
- The network might be slow.

After you resolve the issue, you should close the Scan Status document, and perform scan now again.

If Symantec Mail Security for Domino can confirm that the connection with NNTASK has failed, you receive the following error message:

```
Error communicating with NNTASK. Click Close and try again.
```

After you close the Scan Status document, you can perform scan now again.

LiveUpdate status errors

When you perform an on-demand LiveUpdate, you can check the status of the LiveUpdate to ensure that the most current virus definitions were installed.

See “Updating virus protection with LiveUpdate” on page 185.

When a LiveUpdate status cannot be determined because of an unresponsive server, you receive the following error message:

```
Waiting for response from server. Click “Check LiveUpdate Status”
again. (When no response occurs after 5 minutes, a communication
error with NNTASK might have occurred. See documentation for more
information).
```

When you receive this message, one of the following events might have occurred:

- NNTASK might be under a heavy load and unable to immediately respond to the user’s status request.
- NNTASK might not be running on the server.
- The network might be slow.
- Multiple LiveUpdate sessions might have been triggered on the same server.

  LiveUpdate might take several minutes to complete. LiveUpdate takes longer when multiple sessions are running on the same server.

After you resolve the issue, you should close the LiveUpdate Status document, and run LiveUpdate again.

If Symantec Mail Security for Domino can confirm that the connection with NNTASK has failed, you receive the following error message:

```
Error communicating with NNTASK. Click Close and try again.
```

When you receive this message, you should close the LiveUpdate Status document, and run LiveUpdate again.

Initiating tasks from the Domino console

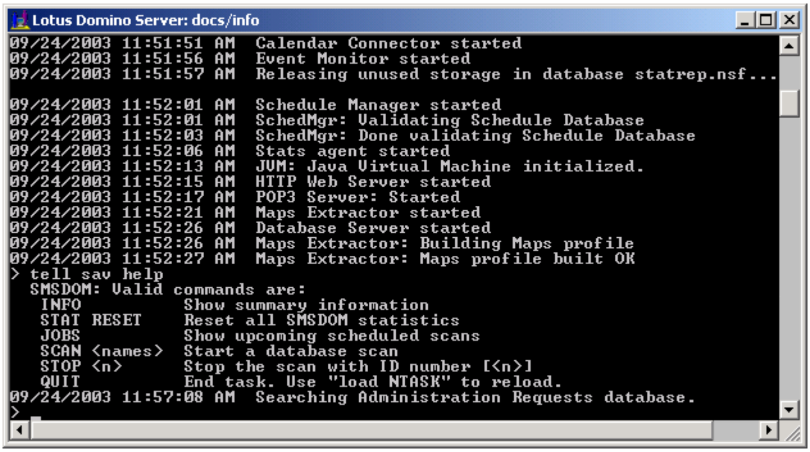
Symantec Mail Security for Domino lets you view, manage, and perform various functions directly from the Domino console. From the console, you can perform on-demand scans that use your Settings database configurations.

Performing tasks from the Domino console

You can manage several Symantec Mail Security for Domino operations and perform scanning functions from the Domino server console.

Figure 2-3 shows the Domino server console.

Figure 2-3 Domino console



```
09/24/2003 11:51:51 AM   Calendar Connector started
09/24/2003 11:51:56 AM   Event Monitor started
09/24/2003 11:51:57 AM   Releasing unused storage in database statrep.nsf...

09/24/2003 11:52:01 AM   Schedule Manager started
09/24/2003 11:52:01 AM   SchedMgr: Validating Schedule Database
09/24/2003 11:52:03 AM   SchedMgr: Done validating Schedule Database
09/24/2003 11:52:06 AM   Stats agent started
09/24/2003 11:52:13 AM   JVM: Java Virtual Machine initialized.
09/24/2003 11:52:15 AM   HTTP Web Server started
09/24/2003 11:52:17 AM   POP3 Server: Started
09/24/2003 11:52:21 AM   Maps Extractor started
09/24/2003 11:52:26 AM   Database Server started
09/24/2003 11:52:26 AM   Maps Extractor: Building Maps profile
09/24/2003 11:52:27 AM   Maps Extractor: Maps profile built OK
> tell sav help
  SMSDOM: Valid commands are:
   INFO          Show summary information
   STAT RESET    Reset all SMSDOM statistics
   JOBS          Show upcoming scheduled scans
   SCAN <names>  Start a database scan
   STOP <n>      Stop the scan with ID number [<n>]
   QUIT          End task. Use "load NTASK" to reload.
09/24/2003 11:57:08 AM   Searching Administration Requests database.
>
```

Table 2-4 lists the commands that you can use from the Domino console.

Table 2-4 Console commands

Command	Description
HELP	Lists Symantec Mail Security for Domino console commands.
INFO	Provides a summary of Symantec Mail Security for Domino operations.
STAT RESET	Clears processing details.
JOBS	Lists upcoming scheduled scans by job name. The job name is the description given to the scheduled scan. See "About scheduled scanning" on page 174.

Table 2-4 Console commands

Command	Description
SCAN <database>	Initiates a scan of the specified databases. A number is displayed in the console to identify each scan. When no databases are specified, only databases in the default data directory are scanned. (No subdirectories are scanned.) You can specify databases with long file names, but the file names must not have spaces.
STOP <n>	Stops a specific scan. When you perform a scan, the scan is assigned a number. You can find the scan number in the Log in Server Messsages or in the Domino server console.
QUIT	Stops the Symantec Mail Security for Domino server process. Type LOAD NNTASK at the console command prompt to reload Symantec Mail Security for Domino. If you have the premium antispam service enabled, stopping the Symantec Mail Security for Domino server process will also stop the flow of incoming SMTP traffic. To continue the flow of SMTP traffic, you must disable the premium antispam service before you stop the Symantec Mail Security for Domino server process. See "Enabling and disabling the premium antispam service" on page 159.

To perform tasks from the Domino console

- At the command prompt, type **`TELL SAV`** <command>

Performing on-demand scanning from the Domino server console

When you perform an on-demand scan from the server console, Symantec Mail Security for Domino uses the configurations that you defined in the Settings database on Scan Now tab. However, you can use scan commands to modify how Symantec Mail Security for Domino disposes of documents that contain violations.

The scan commands that you type at the console differ depending on how you want to dispose of a document that contains a scanning violation.

Table 2-5 lists the scan commands that you can use to dispose of documents that contain violations.

Table 2-5 Document violation scan commands

Command	Description
A	Action: Perform an action.
D	Delete: Delete documents that contain a violation.
N	Ignore: Log the violation, but do nothing with the document.
Q	Quarantine: Quarantine documents that contain violations.
R	Repair: Repair documents that contain violations.
U	Unrepairable: Dispose of unrepairable documents. (You must specify how to dispose of unrepairable documents.)

When you configure Symantec Mail Security for Domino to attempt to repair an infected document, you must also specify what action to take when the document cannot be repaired.

Table 2-6 lists the scan commands that you can use to dispose of unrepairable documents.

Table 2-6 Unrepairable document scan commands

Command	Description
D	Delete: Delete documents that contain a violation.
N	Ignore: Log the violation, but do nothing with the document.
Q	Quarantine: Quarantine documents that contain violations.

If you do not specify an unrepairable document scan command, Symantec Mail Security for Domino uses the settings that are defined on the Scan Now > What to Scan tab.

When Symantec Mail Security for Domino detects a virus inside of a container file, it might delete the container file and everything in it. When a container file is comprised of both infected and uninfected files, the entire container file and all of the files inside it might be deleted.

To scan documents using Scan Now tab settings

- At the command prompt type:

  ```
  TELL SAV SCAN <database>
  ```

To scan documents without attempting to repair infected documents

- At the command prompt type:

  ```
  TELL SAV SCAN /A<scan command> <database>
  ```

  For example, to scan the InfoDocs database and quarantine any violations, at the command prompt type:

  ```
  TELL SAV SCAN /AQ INFODOCS
  ```

To scan documents and attempt to repair infected documents

- At the command prompt type:

  ```
  TELL SAV SCAN /AR  /U<scan command> <database>
  ```

  For example, to scan the InfoDocs database, attempt to repair infected documents, but delete files that cannot be repaired, at the command prompt type:

  ```
  TELL SAV SCAN /AQ /UD INFODOCS
  ```

Uninstalling Symantec Mail Security for Domino

Symantec Mail Security for Domino includes a setup option that lets you retain existing Symantec Mail Security for Domino databases.

Before you uninstall the product, you must uninstall the SESA Agent if it is installed on your computer. You must also disable Symantec Premium AntiSpam if it is enabled.

See “Enabling and disabling the premium antispam service” on page 159.

See “Uninstalling the local SESA Agent” on page 249.

You can also uninstall Symantec Mail Security for Domino from the Control Panel by using the Add/Remove Programs option.

To uninstall Symantec Mail Security for Domino

1. If a Notes client is running on the server, close the client.
2. Turn off the Lotus Domino server.
3. On the Domino server on which Symantec Mail Security for Domino is installed, on the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for Domino** > **Uninstall Symantec Mail Security for Domino**.
4. In the confirmation window, click **Yes**.

5 When prompted to keep existing Symantec Mail Security for Domino databases and statistics, select the database and statistic descriptions that you want to keep.

6 When the uninstallation is complete, in the Remove Programs From Your Computer dialog box, click **OK**.

Chapter 3

Activating your Symantec Mail Security for Domino licenses

This chapter includes the following topics:

- About licensing
- About license activation
- If you want to renew a license

About licensing

Key features for Symantec Mail Security for Domino, which include scanning functionality and virus definitions updates, are activated by a license. When a license expires or no license is installed, limited functionality is available. To regain product functionality when your license expires, you must renew and reactivate your license subscription.

For complete scanning functionality and product and virus definitions updates, you need the following licenses:

Product license	A product license is required to activate Symantec Mail Security for Domino scanning operations. Scanning operations include virus scanning, content filtering, and antispam scanning (standard antispam and the premium antispam service). See "About scanning" on page 167.

Content license	A content license is required to update Symantec corporate software with the latest associated content, such as new virus definitions, through LiveUpdate. A valid content license ensures that servers remain protected with the latest virus definitions. See "About LiveUpdate" on page 181.
Symantec Premium AntiSpam license	This license is required to enable Symantec Premium AntiSpam. Symantec Premium AntiSpam is a subscription service that provides enhanced spam detection. Continuous updates to the premium antispam filters ensure that your Domino server has the most current spam detection filters that are available. Without this license, the premium antispam service does not function. The Symantec Premium AntiSpam license does not affect the standard antispam feature. The standard antispam feature is enabled through the Symantec Mail Security for Domino product license. See "Identifying spam using the premium antispam service" on page 157.

A license affects the relevant behavior only. For example, when the product license is missing or invalid, you can access the interface to view and modify settings and run reports, but you cannot perform any of the scanning functions. When a content license is missing or invalid, you cannot download virus definitions updates to keep protection current. When the premium antispam service license is missing or invalid, the premium antispam service does not function.

See "About license activation" on page 62.

Virus definitions updates and scanning operations are limited to the period of time that is specified by the respective license. The start and end dates of the license period depend on the terms of your license agreement. When a license approaches its expiration date, it enters the warning period. During the warning period, the product sends messages to remind you that your license needs to be renewed.

See "If you want to renew a license" on page 71.

About license activation

Symantec issues a serial number for each type of license that you purchase. This serial number is required to register your product and your maintenance agreement. The serial number is provided on a license certificate, which is mailed separately and arrives in the same time frame as your software. For security reasons, the license certificate is not included in the Symantec Mail

Security for Domino software distribution. If you are upgrading from a previous version of the product and you have an active maintenance contract, you might receive the serial number certificate with an upgrade insurance letter.

See "If you do not have a serial number" on page 63.

License activation involves the following process:

Obtain a license file from Symantec.	To request a license file, you must have the license serial number for each license that you want to activate. After you complete the registration process, Symantec sends you the appropriate license file by email. See "Obtaining a license file" on page 63.
Install the license file.	You must install the content and product licenses on each server on which you run Symantec Mail Security for Domino. This enables the scanning processes and lets you update your product and its associated content using LiveUpdate. See "Installing product and content license files" on page 65. If you purchased a subscription for the Symantec Premium AntiSpam service, you must install the Symantec Premium AntiSpam license on the servers on which you intend to use the premium antispam service. See "Installing a Symantec Premium AntiSpam license file" on page 67.

If you do not have a serial number

Your license certificate, which contains the serial numbers for the licenses that you have purchased, should arrive within three to five business days of when you receive your software or subscribe to Symantec Premium AntiSpam. If you do not receive the license certificate, contact Symantec Customer Service at 800-721-3934 or your reseller to check the status of your order. If you have lost your license certificate, contact License Support.

See "Where to get more information about Symantec Mail Security for Domino" on page 28.

Obtaining a license file

To request a license file, you must have the serial number that is required for activation. (Each license has a separate serial number.) The serial number is used to request a license file and to register for support.

The serial number is printed on the license certificate that was mailed to you. The format of a serial number is a letter followed by 10 digits, for example, F2430482013.

See "If you do not have a serial number" on page 63.

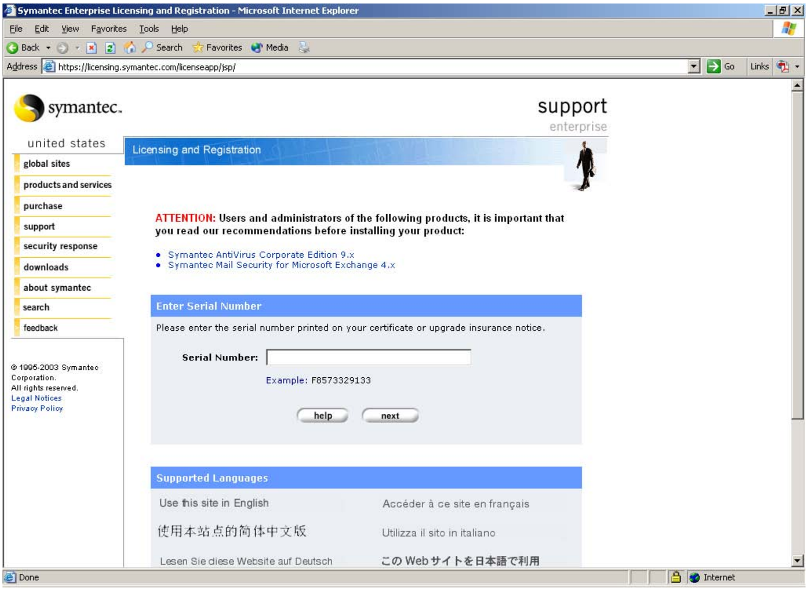
If you purchased multiple types of licenses but register them separately, Symantec sends you a separate license file for each license. You must install each license file separately. If you register multiple licenses at the same time, Symantec sends you a single license file that contains all of your licences.

The license file that Symantec sends to you is contained within an attached .zip file. The .slf file that is contained within the .zip file is the actual license file. You should ensure that your inbound email environment permits .zip email message attachments.

Warning: License files are digitally signed. If you attempt to edit a license file, you will corrupt the file and render it invalid.

To obtain the license file

1 In a Web browser, type the following address:
https://licensing.symantec.com



Address: https://licensing.symantec.com/licenseapp/jsp/

ATTENTION: Users and administrators of the following products, it is important that you read our recommendations before installing your product:

- Symantec AntiVirus Corporate Edition 9.x
- Symantec Mail Security for Microsoft Exchange 4.x

Enter Serial Number

Please enter the serial number printed on your certificate or upgrade insurance notice.

Serial Number:

Example: F8573329133

Supported Languages

Use this site in English | Accéder à ce site en français
使用本站点的简体中文版 | Utilizza il sito in italiano
Lesen Sie diese Website auf Deutsch | この Webサイトを日本語で利用

© 1995-2003 Symantec Corporation.
All rights reserved.
Legal Notices
Privacy Policy

Your Web browser must use 128-bit encryption to view the site.

2 In the Serial Number box, type the 11-digit serial number that is provided on the license certificate, and then click **Next**.

If you are registering multiple types of licenses, type one of the serial numbers, and then click **Next**. Follow the on-screen instructions to add additional serial numbers.

3 Follow the on-screen instructions to register your license and receive your license file.

Symantec will send you an email message that contains the license file in an attachment. If the email message does not arrive within two hours, an error might have occurred, such as an invalid email address entry. You should try again to obtain the license file through the Symantec Web site.

Installing product and content license files

A license file contains the information that is required to activate one or more features in a product or to update the product and its associated content. A license file may contain one or more types of licenses, depending on whether you registered the license serial numbers separately or at the same time.

Symantec Mail Security for Domino requires a product license and a content license to ensure proper functionality. To activate the premium antispam service, you also must have a Symantec Premium AntiSpam license. Additional configuration is required to ensure proper functionality.

See “Installing a Symantec Premium AntiSpam license file” on page 67.

You must install the product and content license files on each server on which Symantec Mail Security for Domino is installed, regardless of whether the Domino installation is partitioned or the Domino server is a cluster member. For example, if the server has multiple partitions, you only need to install one content license file and one product license file on the server. Likewise, you must install one content license file and one product license file on each member of a cluster.

A license file cannot be replicated. You can install a license file on one or more servers within a server group at one time.

After you activate a content or product license, you can check the license status and configure the product to notify you when the license is about to expire.

See “Checking the license status” on page 70.

See “Receiving notification when a license is about to expire” on page 70.

Note: If you are upgrading to Symantec Mail Security for Domino from Symantec AntiVirus/Filtering for Domino 3.1, you must install the product and content licenses for the product to be fully functional.

To install product and content license files

1. When you receive the email message from Symantec that contains the license file, save the license file to a location that is easily accessible.
   The file is delivered as a .zip file. You must extract the file contents from this file.
2. On the Lotus Notes client, open the Symantec Mail Security for Domino Settings database.
3. In the Settings view, double-click the server group on which you want to install the license.
4. On the Licensing tab, on the Action bar, click **Install or Upgrade License**.
5. In the Install or Upgrade License window, on the License tab, select the servers in the server group on which you want to install the license.
   All of the servers in the group are selected by default.
6. Click **Browse** to locate the license file.
   The license file has a .slf extension.
7. In the Select the license file dialog box, select the license file, and then click **Open**.
8. Click **OK**.
9. On the License Installation Status document, on the Action bar, click **Check License Installation Status**.
10. Verify whether the license file installed successfully, and then do one of the following:
    - If the license installed successfully, on the Action bar, click **Close**.
    - If the license file did not install successfully, resolve the errors and then reinstall the license file.
      See “License installation status errors” on page 53.

Installing a Symantec Premium AntiSpam license file

To enable antispam scanning functionality, you must activate a product license. To enable the premium antispam service, you must also activate the Symantec Premium AntiSpam license.

You must install the license file before you enable the premium antispam service. You only need to install the Symantec Premium AntiSpam license on the servers on which you intend to use the premium antispam service. Installing a license file that includes the Symantec Premium AntiSpam license on a server that is not configured to use the premium antispam service does not affect server performance nor does it enable the premium antispam service.

See “Installing product and content license files” on page 65.

If you register the premium antispam service license separately from the content and product licenses, you receive a separate license file for Symantec Premium AntiSpam. You must install this license file separately. If you register all of the licenses simultaneously, you receive one license file. You must install this license file on all servers that require any of the licenses that are contained in the license file.

See “Obtaining a license file” on page 63.

Internet access for the server is required to activate the license and to receive updated filtering rules. Updates to the premium antispam service are handled through the Symantec Premium AntiSpam service and not through LiveUpdate. To install and activate the premium antispam service license on a server that is behind a firewall, you must provide the information that is needed to connect to the proxy server that handles Internet traffic for that server or server group.

You can install a license file on one or more servers within a server group at one time. If you are installing the license file on multiple servers at the same time and these servers use a proxy server for Internet access, then you should install the license file by server group and by proxy settings.

See “After you install the Symantec Premium AntiSpam license file” on page 69.

Note: Symantec Premium AntiSpam does not support the installation of license files from path names that contain high ASCII or double-byte characters.

To install a Symantec Premium AntiSpam license file

1 When you receive the email message from Symantec that contains the license file, save the license file to a location that is easily accessible.

The file is delivered as a .zip file. You must extract the file contents from this file.

2. On the Lotus Notes client, open the Symantec Mail Security for Domino Settings database.
3. In the Settings view, double-click the server group on which you want to install the license.
4. On the Licensing tab, on the Action bar, click **Install or Upgrade License**.
5. In the Install or Upgrade License window, on the License tab, select the servers in the server group on which you want to install the license.
   All of the servers in the group are selected by default.
6. Click **Browse** to locate the license file.
   The license file has a .slf extension.
7. In the Select the license file dialog box, select the license file, and then click **Open**.
8. If the servers on which you want to install the license file connect to the Internet through a proxy server, on the Proxy tab, configure the proxy settings as follows:

Host

Type the host name or IP address of the server that is used to access the Internet.

This information must be the same for all of the servers that you select.

Port

Type the port number that is used to access the proxy server. If no information is provided, the default port number 1080 is used.

This information must be the same for all of the servers that you select.

User Name

Type the user name that is required to log on to the proxy server.

This information must be the same for all of the servers that you select. Leave this field blank if no user name is required.

Password

Type the password that is required to log on to the proxy server, if needed.

This information must be the same for all of the servers that you select. Leave this field blank if no user name is required.

To secure the transmission of your password over the network, you should encrypt the network port data. Click **Set Port Preferences** to configure or check port settings.

9 Click **OK**.

10 On the License Installation Status document, on the Action bar, click **Check License Installation Status**.

11 Verify whether the license file installed successfully, and then do one of the following:

- If the license installed successfully, on the Action bar, click **Close**.
- If the license file did not install successfully, resolve the errors and then reinstall the license file.

  See "License installation status errors" on page 53.

After you install the Symantec Premium AntiSpam license file

To use Symantec Premium AntiSpam, you must enable the premium antispam service.

See "Enabling and disabling the premium antispam service" on page 159.

After you activate the premium antispam service license, if you change the proxy server settings for the server on which the premium antispam service is enabled, you must reinstall the premium antispam service license and specify the new proxy settings. Otherwise, the premium antispam service is unable to update the spam detection filters.

You can check the license status and configure the product to notify you when the license is about to expire.

See "Checking the license status" on page 70.

See "Receiving notification when a license is about to expire" on page 70.

If your premium antispam service license expires, the premium antispam service is automatically disabled. After you activate your new license, you must re-enable the premium antispam service.

See "If you want to renew a license" on page 71.

See "Enabling and disabling the premium antispam service" on page 159.

Checking the license status

You can check the status of your product, content, and premium antispam service licenses from the Lotus Notes client or from the Domino server console. You can use this information to verify that your licenses are current and that your product is activated and protecting your computers.

To check the license status from the Lotus Notes client

- Do one of the following:
  - In the Log database, in the left pane, click **Server Messages**.
  - In the Settings database, in the Group document, on the Action bar, click **Show Server Status**, and then click **Check Statistics**.
    See "Checking server status" on page 51.

To check the license status from the Domino server console

- On the Domino server console, at the command prompt, type the following:
  ```
  TELL SAV INFO
  ```

Receiving notification when a license is about to expire

Virus definitions updates and scanning operations are limited to the period of time that is specified by the respective license. When a license approaches its expiration date, it enters the warning period. You can configure the product to send you a message to remind you that your license needs to be renewed.

To receive notification when a license is about to expire

1. On the Lotus Notes client, open the Symantec Mail Security for Domino Settings database.
2. In the Settings view, double-click a server group.
3. In the Group document, on the LiveUpdate tab, on the Notifications tab, under When to notify, check **When license enters warning period or is expired notify me every [14] days**.
   The default setting is 14, but you can change the number of days.
4. In the Specified users to notify list, select who to notify when the license is about to expire.
5. On the Action bar, click **Save**.

If you want to renew a license

When a server has an expired premium antispam service license or when the premium antispam service license is missing or invalid, the premium antispam service is disabled. After you receive and activate a new Symantec Premium AntiSpam license, you must re-enable the premium antispam service.

See "Enabling and disabling the premium antispam service" on page 159.

When a server has an expired content license or when the content license is missing or invalid, content updates are not applied to your product, which can leave your server vulnerable to virus attacks. When a content license expires, you must renew your Maintenance Agreement to receive content updates.

The process for license renewal depends on how you purchased your software.

If you purchased Symantec Mail Security for Domino through the Symantec Value or Elite Enterprise Licensing programs	To determine whether your Maintenance Agreement has been renewed and if new licenses are available, contact your administrator or reseller. After your Maintenance Agreement is renewed, you receive new serial numbers that you can register to obtain your new license files.
If you purchased Symantec Mail Security for Domino Small Business Edition	For more information about license renewal, visit the following Web site: http://www.symantecstore.com/renew

Administering Symantec Mail Security for Domino on multiple servers

This chapter includes the following topics:

- About administering Symantec Mail Security for Domino on multiple servers
- Managing multiple servers
- Customizing server groups

About administering Symantec Mail Security for Domino on multiple servers

You can simplify the creation and management of Symantec Mail Security for Domino databases across multiple Lotus Domino servers. Choose a single server on which to manage Symantec Mail Security for Domino and receive updated virus definitions. Use Lotus Domino replication technology to synchronize the Symantec Mail Security for Domino databases on the managed server with other servers. You can also use the replication process to send statistics and reports on incidents for all of the servers to the managed server.

See "Managing multiple servers" on page 74.

For more information about database replication, see your Lotus Domino documentation.

Use server groups to simplify the management of your servers. Create server groups that have a common purpose and, therefore, require the same protection (for example, email servers). By grouping servers, you apply a common set of protection settings once, rather than repeatedly to each server. In a large network with multiple servers that perform similar roles, the reduction in configuration time and maintenance costs can be considerable.

See "Customizing server groups" on page 79.

Managing multiple servers

You can simplify the management of multiple Lotus Domino servers when you replicate the Symantec Mail Security for Domino databases.

The benefits of database replication are as follows:

- Configure and manage the product from one location.
- Ensure that all servers are configured exactly the same.
- Update virus definitions from one server.
- Collect and view reports and statistics for all servers in the managed server's Log.

See "About replicating Symantec Mail Security for Domino databases" on page 74.

You can create replica databases on your additional servers using one of the following methods:

- Create the database replicas on additional servers before you install Symantec Mail Security for Domino.
- Create the database replicas on additional servers after you install Symantec Mail Security for Domino.

If you intend to replicate the Definitions database, you must first configure the Settings database options.

See "Creating replica databases on an additional server" on page 76.

About replicating Symantec Mail Security for Domino databases

To replicate Symantec Mail Security for Domino databases across multiple servers, you must first select a specific computer to host the hub for the databases. Then, you must create replicas of the databases on your additional servers. (The replicas must have the same names as the hub databases.) With Lotus Domino push-pull replication technology, data on the hub is copied to the corresponding databases on the additional servers.

For more information about replication procedures, see the appropriate Lotus Domino documentation.

Ensure that you replicate Symantec Mail Security for Domino databases only to other servers that are running the same version of Symantec Mail Security for Domino and that are on the same operating system. Undesirable results are likely to occur when you replicate databases that are installed on different product versions or operating systems, and Symantec cannot provide support for this configuration.

You can replicate the following Symantec Mail Security for Domino databases:

- Settings database (sav.nsf)
- Log database (savlog.nsf)
- Quarantine database (savquar.nsf)
- Definitions database (savdef.nsf)

Settings database

Through replication, the Symantec Mail Security for Domino server task, NNtask, monitors the Settings database for changes. Any changes made to the Symantec Mail Security for Domino Settings database on any of the Domino servers are distributed to the other replicas when a manual or scheduled replication occurs. After replication, the new settings are automatically reloaded.

All Settings database options are replicated among the Domino servers.

Note: You can avoid replication save conflicts by permitting only the Domino administrator in charge of antivirus policy to modify the Symantec Mail Security for Domino Settings database on each of the Domino servers.

Log database

Choose a computer to act as the hub for the Log. When you replicate the Log database, the hub receives violation incidents and reports from the other Domino servers that run Symantec Mail Security for Domino.

See “Using the Symantec Mail Security for Domino Log” on page 195.

To centralize logging of violation incidents and reports, initiate pull replication to the Symantec Mail Security for Domino Log hub server from the spoke servers. If you do not need to centralize logging, you may use push-pull replication.

Quarantine database

You can replicate the Quarantine database to create a central repository of quarantined documents, although you might find it unnecessary. The Quarantine database provides access to quarantined and backup documents. Symantec Mail Security for Domino backs up documents before deleting them or attempting to repair infected attachments.

See "About the Quarantine" on page 213.

Definitions database

The Symantec Mail Security for Domino Definitions database stores updated virus definitions. You create the Definitions database only if you plan to replicate updated virus definitions to additional servers. When you replicate the Definitions database, only a single LiveUpdate is required to maintain current antivirus protection on all of your servers.

See "About LiveUpdate" on page 181.

The Domino server that will download new virus definitions through LiveUpdate must be the hub for the Definitions database. The Definitions database stores the active definitions set, as well as the most recent downloaded definitions. Symantec Mail Security for Domino virus definitions are operating system specific.

Creating replica databases on an additional server

When setting up an additional server, you must create replicas of the Symantec Mail Security for Domino databases on each server. During the replication process, the hub server copies the data from its databases to the databases of the same name on the additional servers.

To create replicas of the Settings, Log, and Quarantine databases on an additional server, select one of the following methods:

- Replicate the Symantec Mail Security for Domino Settings, Log, and Quarantine databases from the hub server to the additional server. Then, install Symantec Mail Security for Domino on the additional server, and choose to keep the existing databases when the setup program prompts you.
- Install Symantec Mail Security for Domino on the additional server, and then replicate the Settings, Log, and Quarantine databases from the hub server to the additional server.

If you intend to replicate updated virus definitions to your additional servers, you must also configure Lotus Domino to replicate the Definitions database.

See "Updating virus protection with LiveUpdate" on page 185.

To create replica databases when Symantec Mail Security for Domino is not installed on the additional server

1. Select a server in your organization to be the hub for the Symantec Mail Security for Domino server.
2. Install Symantec Mail Security for Domino on the server, and then start the Domino server on that computer.
3. Create a server group.
   See "Creating a server group" on page 80.
4. Ensure that you (the administrator) and LocalDomainServers are in the Access Control List of sav.nsf and savlog.nsf with Manager access and that Delete Documents is enabled.
   The LocalDomainServers group contains all of the servers to which you plan to replicate.
   See "Setting access control for Symantec Mail Security for Domino databases" on page 43.
5. Create replicas of the newly installed sav.nsf, savlog.nsf, and, if desired, savquar.nsf databases in the <Domino server data directory>\SAV directory on the other Domino servers.
   The Lotus Domino server default data directory is:
   <drive>:\Lotus\Domino\Data\SAV
6. Install Symantec Mail Security for Domino on the other servers, but keep the already replicated sav.nsf, savlog.nsf, and savquar.nsf databases.
   The option to keep existing databases is part of the Symantec Mail Security for Domino installation program.

To create replica databases when Symantec Mail Security for Domino is installed on the additional server

1. On each additional server, in the Domino server console, type the following:

   ```
   TELL SAV QUIT
   ```

2. Replicate the Symantec Mail Security for Domino Settings, Log, and if desired, Quarantine databases from the hub Domino server to the additional Domino servers in the <Domino server data directory>\SAV directory.
3. When you are prompted to overwrite the existing sav.nsf, savlog.nsf, or savquar.nsf databases, click **Yes**.
   This overwrites the existing databases with the new replicas.
4. At each additional server, in the Domino server console, restart Symantec Mail Security for Domino by typing the following:

   ```
   LOAD NNTASK
   ```

To create a replica Definitions database

1. Select a Domino server in your organization to use for downloading updated virus definitions.
2. In the Settings view, double-click the appropriate server group.
3. On the LiveUpdate tab, on the Basics tab, click **Enable LiveUpdate**.
   This option is enabled by default.
4. Check **Save downloaded virus definitions in the SMSDOM Definitions database**.
5. Click **All servers in this group**.
   You must select this option to avoid replication save conflicts.
6. On the Action bar, click **Create SMSDOM Definitions Database** to create the Definitions database.
7. Ensure that you (the administrator) and LocalDomainServers are in the Access Control List of savdefs.nsf with Manager access and that Delete Documents is enabled.
   The LocalDomainServers group contains all of the servers to which you plan to replicate.
   See "Setting access control for Symantec Mail Security for Domino databases" on page 43.
8. Create replicas of the hub for the Definitions database on the other Domino servers that run Symantec Mail Security for Domino.
   The savdefs.nsf database must reside in the <Domino server data directory>\SAV directory on the other Domino servers and must be named savdefs.nsf.

The next time that a scheduled LiveUpdate runs, updated virus definitions are downloaded to the Definitions database. The new virus definitions set is marked as active. The updated definitions are distributed to the other replicas when a manual or scheduled replication occurs.

Customizing server groups

When setting up a server group, you decide which servers belong together and which set of protections to apply to them. For example, you can create a group of servers that are not used for mail routing and turn off email scanning for that group.

See "Creating a server group" on page 80.

An Unassigned Servers server group always exists and contains any servers that are not assigned to a server group. The Unassigned Servers server group cannot be deleted.

After you create a server group, you can copy the settings to create new server groups.

See "Copying settings to create a new server group" on page 81.

If you remove a server from your system or decide to move the server to a different server group, you can remove it from the server group listing. Servers that are listed in the Unassigned Servers server group cannot be deleted.

See "Removing a server from a server group" on page 82.

You can delete an entire server group; however, all of the configuration settings for that group, such as content filtering rules and antispam settings, are also deleted and cannot be restored. The Unassigned Servers server group cannot be deleted.

See "Deleting a server group" on page 82.

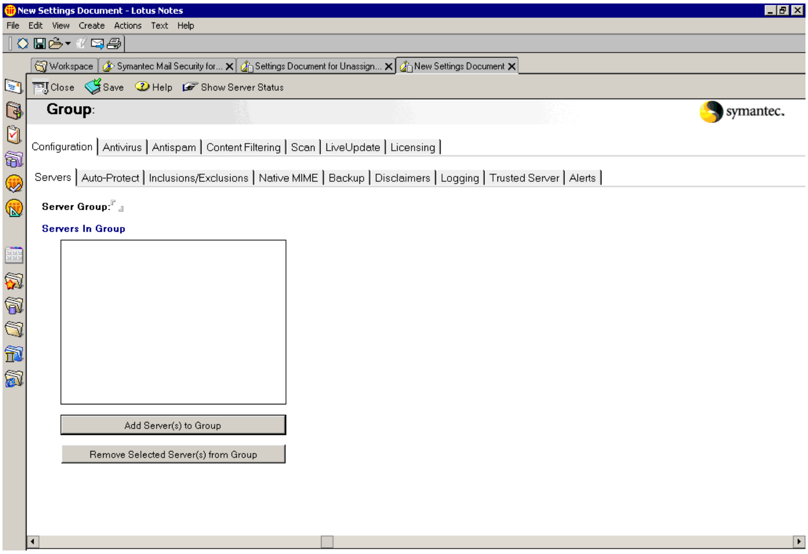
Creating a server group

You can create as many server groups in the Settings database as needed. A server group called Unassigned Servers always exists and contains any servers that are not assigned to another server group. A server can only reside in one server group at a time, and the Unassigned Servers Group cannot be deleted.

To create a server group

1 On the Lotus Notes client, open the Settings database.

2 In the Settings view, on the Action bar, click **New Server Group**.



3 On the Configuration tab, on the Servers tab, beside Server Group, type a name for the server group.

4 Click **Add Server(s) to Group**.

5 In the Add Server to Group dialog box, select one or more servers, and then click **OK**.

6 On the Action bar, click **Save**.

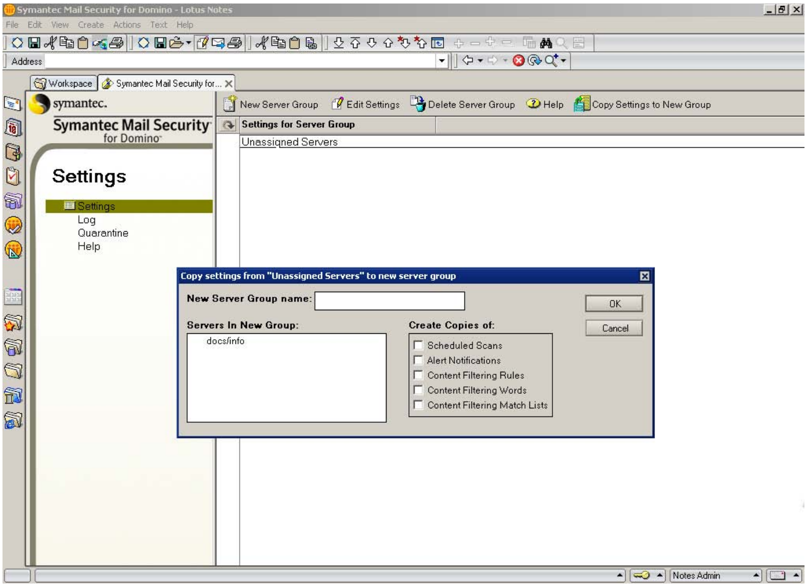
Copying settings to create a new server group

To save time, you can copy the settings that you have configured for one server group to a new server group.

To copy settings to create a new server group

1 In the Settings view, select the server group that you want to copy.

2 On the Action bar, click **Copy Settings to New Group**.


Symantec Mail Security for Domino - Lotus Notes
File Edit View Create Actions Text Help
Address
Workspace
Symantec Mail Security for...
symantec.
Symantec Mail Security for Domino
Settings
Settings
Log
Quarantine
Help
New Server Group
Edit Settings
Delete Server Group
Help
Copy Settings to New Group
Settings for Server Group
Unassigned Servers
Notes Admin

Copy settings from "Unassigned Servers" to new server group

New Server Group name:

Servers In New Group:
docs/info

Create Copies of:
☐ Scheduled Scans
☐ Alert Notifications
☐ Content Filtering Rules
☐ Content Filtering Words
☐ Content Filtering Match Lists

OK
Cancel

3 In the New Server Group name box, type a name for the new server group.

4 Under Servers In New Group, select the servers that you want to add to the group.

5 Under Create Copies of, check the settings that you want to copy to the new server group, and then click **OK**.

6 On the Servers tab, click **Add Server(s) to Group**.

7 Select one or more servers to add to the server group, and then click **OK**.

8 Under Servers In Group, select the servers to remove from the group (if any), and then click **Remove Selected Server(s) from Group**.

9 On the Action bar, click **Save**.

Removing a server from a server group

If you remove a server from your system configuration or you decide to move a server from one server group to another, you can delete the server from an existing server group.

To remove a server from a server group

1. In the Settings view, double-click the server group that contains the server that you want to remove from the server group.
2. Under Servers In Group, select the server that you want to remove from the group.
3. Click **Remove Selected Server(s) from Group**.
4. On the Action bar, click **Save**.

Deleting a server group

You can delete an entire server group from the listing of server groups. When you delete a server group, you delete all of the configuration settings that are associated with the group, such as antivirus settings, content filtering rules, and antispam configurations. These settings cannot be restored after they are deleted. The Unassigned Servers server group cannot be deleted.

To delete a server group

1. In the Settings view, select the server group that you want to delete.
2. On the Action bar, click **Delete Server Group**.
3. In the confirmation window, click **Yes**.

Setting global scanning options

This chapter includes the following topics:

About global scanning options

Symantec Mail Security for Domino lets you customize scanning options. The settings that apply to all scanning for a particular server group are contained within the Settings database on the Configuration tab. Settings that are unique to a specific scan type, such as antivirus, content filtering, or antispam scanning, must be made on the tab for that scan type.

For example, the option to scan all file name extensions is a global setting that applies to all scans and is configured on the Configuration tab. The heuristic virus detection level option only applies to antivirus scanning and is configured on the Antivirus tab.

Configuring global scanning options

Symantec Mail Security for Domino has several global scanning options that you can configure:

Inclusions/ Exclusions	Define which databases and file attachments to scan. See “Specifying what to scan” on page 84.
Native MIME	Customize the MIME message text. See “Customizing the native MIME message” on page 86.
Backup	Set rules for creating backups before repairing or deleting infected documents. See “Creating backup documents” on page 86.
Disclaimers	Define the disclaimer mark and header and footer text. See “Configuring disclaimer options” on page 86.
Logging	Select which information to log and choose the logging destinations. See “Configuring logging options” on page 88.
Trusted Server	Select which servers can bypass scanning processes. See “Configuring trusted server options” on page 89.
Alerts	Configure rules for sending alert notifications. See “Configuring alerts” on page 90.

Specifying what to scan

Symantec Mail Security for Domino lets you choose which databases and directories to scan. You can exclude specific databases or directories from scans that might not be at risk for virus infection or require content filtering. For example, you might have documentation or reference databases that are not at risk because they cannot be modified by users. Symantec Mail Security for Domino databases (sav.nsf, savlog.nsf, savquar.nsf, savhelp.nsf, and savdefs.nsf) are automatically excluded from scans.

By default, Symantec Mail Security for Domino scans all document attachments regardless of extension. This is the most secure setting but imposes the heaviest demand on resources.

You can limit which types of file attachments are scanned by using an inclusion list. You specify the file name extensions that you want to scan in the inclusion list. Only the file types that are listed in the inclusion list are scanned, which can optimize performance. However, this is the least secure configuration because there is an unlimited number of possible file name extensions that are not scanned.

If you configure Symantec Mail Security for Domino to scan attachments using an inclusion list, container files and the files within the container are scanned only if their file name extensions are listed in the inclusion list.

Note: To enhance protection during virus outbreaks, you should scan all files.

To exclude specific databases and directories from scanning

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Inclusions/ Exclusions tab, under Databases, check **Exclude specified databases and directories from scans**.
3. Under Databases and directories to exclude from scans, type the databases and directories that you want to exclude from scanning.
   Separate multiple entries with semicolons (;). Do not use wildcard characters.
4. On the Action bar, click **Save**.

To scan only specific file extensions

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Inclusions/ Exclusions tab, under Attachments, check **Scan attachments with specified file extensions**.
   Scan all attachments regardless of extension is selected by default. This is the most secure setting.
3. Under Specified file extensions, add the file name extensions that you want to scan.
   The default setting is an asterisk (*). When no changes are made to the default setting, the product scans all file extension types.
   Omit the period before the file name extension. Separate multiple entries with semicolons. You can use wildcard characters.
4. On the Action bar, click **Save**.

Customizing the native MIME message

You can configure Symantec Mail Security for Domino to scan for malicious HTML in MIME message bodies. If Symantec Mail Security for Domino detects malicious code in a MIME encoded message, it deletes the entire message body and replaces it. (Infected message bodies cannot be repaired.) You can customize the replacement text message.

To customize the native MIME message

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Native MIME tab, under Replace deleted MIME message bodies with the following text, type your customized message.
3. On the Action bar, click **Save**.

Creating backup documents

When you configure Symantec Mail Security for Domino to repair or delete infected attachments, you have the option to save backup copies of the infected documents to the Quarantine to protect data. In the Quarantine, click Backup documents to view the list and delete or restore backups. (You must have the appropriate Role assignments to view quarantined documents.)

See "Managing backup documents" on page 228.

See "Assigning Quarantine roles" on page 216.

To create backup documents

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Backup tab, under Back up documents before repairing or deleting, check **Yes**.
   See "Upgrading Symantec Mail Security for Domino" on page 35.
3. On the Action bar, click **Save**.

Configuring disclaimer options

Some organizations are required to post disclaimers that indicate that an email message has been scanned. The text that you specify for the disclaimer displays in the header or footer of an email message. When this option is enabled, Symantec Mail Security for Domino inserts your disclaimer in every email message as it passes to its destination.

Disclaimers are only applied to email messages that are sent to or received from addresses that contain different base domains. For example, an email message sent from mailer1@domain.com to mailer2@domain.com would not receive a disclaimer. An email message sent from mailer1@domain.com to mailer3@company.com would receive a disclaimer. The disclaimer is placed on all outgoing email messages for all types of scanning (for example, virus, antispam, or content filtering).

Symantec Mail Security for Domino uses a field called a disclaimer mark to tag email messages. Symantec Mail Security for Domino uses this tag to detect whether a disclaimer message has already been added to the email message. This prevents servers that use the same disclaimer mark from adding the same header or footer message multiple times as an email message passes through routing servers.

The first time that Symantec Mail Security for Domino adds your disclaimer header or footer text to the email message, it also adds your custom disclaimer mark. Choose a unique string that another organization is unlikely to use (for example, your organization's name). You can use one disclaimer mark across all server groups in your organization, or you can use different disclaimer marks for each server group.

To configure disclaimer options

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Disclaimers tab, in the Disclaimer mark box, type the appropriate disclaimer mark.
3. To enable disclaimers, do one of the following:
   - Under Disclaimer headers, check **Enable disclaimer headers**, and then type the text that you want to appear in the disclaimer header.
   - Under Disclaimer footers, check **Enable disclaimer footers**, and then type the text that you want to appear in the disclaimer footer.
4. On the Action bar, click **Save**.

Configuring logging options

You can select which events are logged and to which logging destinations. Symantec Mail Security for Domino automatically logs the events that you designate to the Domino console and the Domino server log.

You can also log events to any of the following locations:

- Symantec Mail Security for Domino Log
  Saves information to the Server Messages view of the Symantec Mail Security for Domino Log
  See "Using the Symantec Mail Security for Domino Log" on page 195.
- Operating System Event Log
  Saves information to the Windows Event Log
- SESA log
  Saves information to the SESA DataStore for viewing from the SESA Console
  See "Application events that are sent to SESA" on page 239.

To configure logging options

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Logging tab, under What to log, select one of the following:
   - General messages
   - General messages and viruses that couldn't be eliminated
   - General messages and all violations
     This option is enabled by default.
3. Under Where to log, select any of the following logging destinations:
   - SMSDOM Log
     This option is enabled by default.
   - Operating System Event Log
   - Enable SESA Logging
     The SESA Agent IP Address [:Port Number] is configured upon software installation.
     The default IP address and port is 127.0.0.1.

   This logging destination is in addition to the console window and Domino server log.
4. On the Action bar, click **Save**.

Configuring trusted server options

Symantec Mail Security for Domino lets you use trusted servers to reduce scanning redundancy and increase performance. A trusted server is one that you know is safe from outside security breaches, by means of a firewall or similar protection device or software, or one that is already scanning email traffic for viruses, spam, and content filtering rule violations.

For example, inside a firewall you might have a number of servers set up to route the same stream of email messages. If every one of those servers scans the same mail stream, you might have unnecessarily redundant scanning processes in place. You can eliminate some of the redundancy by designating servers that Symantec Mail Security for Domino does not have to scan. In this way, you take on a minimal security burden while increasing email delivery performance.

Warning: When you enable the trusted server option, your system might be vulnerable to malicious code attacks. It is important that you maintain current antivirus protection on the trusted servers.

See “Configuring LiveUpdate” on page 181.

To configure trusted server options

1 In the Settings view, double-click a server group.

2 In the Group document, on the Configuration tab, on the Trusted Server tab, under Trust all messages from the following servers, select one of the following:

- Trust no servers: Scans all email messages and document writes from all servers in the server group.
  This option is enabled by default.
- Trust the following servers: Forgoes scanning of email messages that are received from the servers that you specify.

3 If you choose Trust the following servers, do one of the following:

- In the server list, select the servers that should bypass scanning, and then click **OK**.
- Type the server name in abbreviated or canonical format.
  For example:
  MAILHUB1/IT/MYCO or
  CN=MAILHUB1/OU=IT/O=MYCO

Separate entries with commas.

4 On the Action bar, click **Save**.

Configuring alerts

You can configure Symantec Mail Security for Domino to automatically notify administrators when certain violations occur. You can specify which event must occur to trigger the notification, whom to notify, and which statistics to gather.

Symantec Mail Security for Domino lets you notify document recipients and document authors that a violation occurred and how it was handled. You can use tokens to customize your own notification messages to provide further information or instructions. For example, if your policy is to quarantine infected documents, your customized message can inform the intended recipients about who to contact to release the document.

Using tokens to customize email message alerts

To create email message alerts more efficiently, you can substitute tokens to represent custom text.

For example, {green}{18}{italic}{courier} %Author% {black}{normal}{10} displays the author's name in green, 18-point italic type and then returns it to black, 10-point normal type.

Substitution tokens use different delimiters than formatting tokens. You offset substitution tokens with the percentage character (%). You offset format tokens with braces ({}).

Note: Tokens that contain the percentage character (%) are used for the subject and body of the email message. Tokens that contain braces ({}) are only used for the email message body.

Table 5-1 describes the tokens that you can use to customize email message alerts.

Table 5-1 Email message alert tokens

Token	Description
%DBName%	Document's database name.
%DBTitle%	Document's database title.
%DocumentUniqueID%	Unique ID of the document (UNID).
%NoteID%	NOTEID of the document.
%Author%	Most recent author of the document.
%Created%	Creation time and date of the document.

Table 5-1 Email message alert tokens

Token	Description
%Modified%	Time and date of last modification to the document.
%Accessed%	Time and date that the document was last accessed.
%InfectedAttachment%	Name of the first infected attachment.
%Virus%	Name of the first virus found.
%<fieldname>%	Value of the <fieldname> in the document. When a document does not contain a specified field, leave the token blank.
%<servername>%	Name of the Lotus Domino server.
{<font style>}	Value of the font style. The following values are available: Normal, bold, italic, underlined, strikeout, superscripted, subscripted, effect, shadowed, emboss, and extruded. For example, {bold}.
{<font color>}	Value of the font color. The following values are available: Black, white, red, green, blue, magenta, yellow, cyan, dkred, dkgreen, dkblue, dkmagenta, dkyellow, dkcyan, gray, and ltgray. For example, {magenta}.
{<font face>}	Value of the font face. The following values are available: Times, helvetica, and courier. For example, {times}.
{<font size>}	Value of the font size in whole numbers. For example, {24}.

Configuring alert options

Symantec Mail Security for Domino lets you define alerts for different conditions. For example, you can configure Symantec Mail Security for Domino to notify you when it cannot eliminate a virus and has quarantined the document, but not to notify you when it is able to repair a file.

In addition, you can specify a user address for the return address for alerts so that the server is not the recipient of return messages that require action. When the server is the recipient for alerts, the alerts are often undeliverable and result in Delivery Failure Reports (dead mail).

You can log individually named alert statistics to the Lotus Domino Events Log. In addition, you can log virus and content filtering rule violation alerts to the Statistics view of the Symantec Mail Security for Domino Log. This gives you more information about the types of alerts that Symantec Mail Security for Domino generates.

The Symantec Mail Security for Domino and Lotus Domino Logs store an aggregate total of detected virus or content filtering rule violations. You can sort Symantec Mail Security for Domino alerts into finer classes and store individual statistics based on these classes, and you can set up administrator notifications based on these statistics.

To create or modify an alert, configure the following options:

- Basics: Sets the basic options for the alert
- Alert Condition: Sets the conditions for which Symantec Mail Security for Domino generates an alert
- Alert Messages: Sets notification options for the administrator, document author, and document recipients
- Statistics: Sets the options to gather alert statistics

When you no longer need an alert, you can delete it from the list of alerts.

To create or modify an alert

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Alerts tab, do one of the following:
   - Double-click an existing alert to modify it.
   - On the Action bar, click **New Alert** to create a new alert.

To set basic alert options

1. In the Alert Notification document, on the Basics tab, click **Enable this alert** to enable the alert that you are configuring.
   This option is enabled by default.
2. Under Description, type a unique description so that you can identify it in the Alerts view.

3 Under Servers, This alert is valid for, select one of the following:

- All servers in this group: Generates alerts for every server in the selected server group.
  This option is enabled by default.
- The following servers: Generates alerts for only the servers that you select in the drop-down list.
  Separate multiple entries with commas.

4 Under Email address from which the alerts are sent, in the drop-down list, select the return address of an administrator who can act on response messages.

5 On the Action bar, click **Save**.

To set alert condition options

1 In the Alert Notification document, on the Alert Condition tab, under Scan Type, select any of the following:

On-Demand	Selects the alerts that are generated by violations that are found during scan now (on-demand) scans
Scheduled	Selects the alerts that are generated by violations that are found during scheduled scans
Real Time Mail	Selects the alerts that are generated by violations that are found during auto-protect scans of email messages
Real Time Writes	Selects the alerts that are generated by violations that are found during auto-protect scans of database writes

2 To specify the parts of documents for the alert, under Violation Area, select any of the following:

Attachment
Selects the alerts that are caused by violations in email message attachments.

Subject
Selects the alerts that are caused by violations in the email message subject line.

The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Subject).

Body
Selects the alerts that are caused by violations in the body of email messages.

The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Body).

3 To specify the nature of the violation, under Violation Type, select any of the following:

File Name
Selects the alerts that are caused by file name violations.

The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Attachment name).

Document Size
Selects the alerts that are caused by violations in document size.

The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Size or Attachment size).

Author
Selects the alerts that are caused by violations in document authors.

The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Sender).

Virus
Selects the alerts that are caused by viruses that are found in documents or attachments.

Scan Error
Selects the alerts that are caused by scan error violations that are found during antivirus scanning. (Attachments that exceed any of the container limits or are encrypted container files are reported as scan error violations.)

Content	Selects the alerts that are caused by violations in the contents of documents or attachments. The violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified attribute is Body).

4 To specify the action that was taken when a violation was detected, under Action Taken, select any of the following:

Ignored document	Selects the alerts that are generated from documents on which Symantec Mail Security for Domino only logs the event, but does not act.
Copied document	Selects the alerts that are generated from documents that Symantec Mail Security for Domino copies to the Quarantine database after it detects a violation. You must select the Copy the document option on the Content Filtering > Action tab when you configure the content filtering rule for the violation.
Cleaned document	Selects the alerts that are generated from documents that Symantec Mail Security for Domino repairs. The alerts are generated by scans that are configured to repair the infected attachments. You configure this option on the Antivirus > Actions tab.
Removed attachment/ document	Selects the alerts that are generated from documents or attachments that Symantec Mail Security for Domino deletes. The alerts are generated by scans that are configured to delete infected attachments. You configure this option on the Antivirus > Actions tab. Alerts might also be generated by content filtering rule violations for which any delete option is specified on the Content Filtering > Action tab.
Quarantined document	Selects the alerts that are generated from documents or attachments that Symantec Mail Security for Domino quarantines. The alerts are generated by scans that are configured to quarantine infected documents. You configure this option on the Antivirus > Actions tab. Alerts might also be generated by content filtering rule violations for which the Quarantine the document option is selected on the Content Filtering > Action tab.

5 Under Document Origin, select any of the following:

Internet	Selects the alerts that are generated from documents that originate from the Internet. The document violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified Attribute is Internet Domain).
Notes	Selects the alerts that are generated from documents that originate from a local Domino server or domain. The document violation must match the conditions that are specified in the content filtering rule (on the Content Filtering > Rule tab, where the specified Attribute is Domino Domain or Domino Server).

All alert conditions are enabled by default.

Select all selects every option under each alert condition. Deselect all clears every option under each alert condition.

6 On the Action bar, click **Save**.

To set alert message options for administrators

1 In the Alert Notification document, on the Alert Messages tab, on the Administrator tab, click **Send following alert to specified administrators**.
This option is enabled by default.

2 Under Specified administrators, in the drop-down list, select the administrators and others to notify when Symantec Mail Security for Domino detects a virus or rule violation.

3 Under Custom text to specified administrators, in the Subject field, type the subject line of the email message for the alert.
The default text is: SMSDOM detected a violation in a document authorized by %Author%.
Use tokens to customize the subject or body of the email message alert, as necessary.
See "Using tokens to customize email message alerts" on page 90.

4 In the Body field, type the body of the email message for the alert.
The default text is: Please check the SMSDOM Log for more information.
Use tokens to customize the subject or body of the email message alert, as necessary.
See "Using tokens to customize email message alerts" on page 90.

5 To include the action that was taken by Symantec Mail Security for Domino in the email message alert to the administrator, click **Report action taken by Symantec Mail Security for Domino**.
This option is enabled by default.

6 To include information about the violation from the Log in the email message, click **Include violation information from the log**.
This option is enabled by default.

7 On the Action bar, click **Save**.

To set alert message options for the document author

1 In the Alert Notification document, on the Alert Messages tab, on the Document Author tab, check **Send following alert to document author**.

2 Under Custom text to document author, in the Subject field, type the subject line of the email message for the alert.
The default text is: SMSDOM detected a violation in a document you authored.
Use tokens to customize the subject or body of the email message alert, as necessary.
See “Using tokens to customize email message alerts” on page 90.

3 In the Body field, type the body of the email message for the alert.
The default text is: Please contact your system administrator.
Use tokens to customize the subject or body of the email message alert, as necessary.
See “Using tokens to customize email message alerts” on page 90.

4 To include the action that was taken by Symantec Mail Security for Domino in the email message alert to the document author, click **Report action taken by Symantec Mail Security for Domino**.
This option is enabled by default.

5 To include information about the violation from the Log in the email message, click **Include violation information from the log**.
This option is enabled by default.

6 On the Action bar, click **Save**.

To set alert message options for the document recipient

1. In the Alert Notification document, on the Alert Messages tab, on the Document Recipient tab, check **Send following alert to intended recipients**.
2. Under Custom text to document recipients, in the Subject field, type the subject line of the email message for the alert.

   The default text is: SMSDOM detected a violation in a document sent to you.

   Use tokens to customize the subject or body of the email message alert, as necessary.

   See "Using tokens to customize email message alerts" on page 90.
3. In the Body field, type the body of the email message for the alert.

   The default text is: SMSDOM has detected a violation. Please contact your system administrator.

   Use tokens to customize the subject or body of the email message alert, as necessary.

   See "Using tokens to customize email message alerts" on page 90.
4. To include the action that was taken by Symantec Mail Security for Domino in the email message alert to the document recipient, click **Report action taken by Symantec Mail Security for Domino**.

   This option is enabled by default.
5. To include information about the violation from the Log in the email message, click **Include violation information from the log**.

   This option is enabled by default.
6. On the Action bar, click **Save**.

To set alert statistics options

1. In the Alert Notification document, on the Statistics tab, check **Gather statistics for this alert**.

   This option lets you gather statistics in the Lotus Domino Events Log for the particular alert that you are configuring.

   If you enable this option, you must specify the name of the alert statistic and an alert threshold.
2. Under Statistic alert threshold, type the number of times that the alert statistic must be logged to the Lotus Domino Log before the administrator receives notification of the statistic.

   You set notification options in the Lotus Notes Statistics and Events database. For more information, see your Lotus Notes documentation.

3 Under Alert statistic name, type the name of the alert statistic.

Symantec Mail Security for Domino prepends the SAV.Alerts prefix to the name that you specify.

4 On the Action bar, click **Save**.

To delete an alert

1 In the Settings view, double-click a server group.

2 In the Group document, on the Configuration tab, on the Alerts tab, double-click the alert that you want to delete.

3 On the Action bar, click **Delete**.

4 In the confirmation dialog box, click **Yes**.

Establishing antivirus protection

This chapter includes the following topics:

- About antivirus protection
- Establishing antivirus scanning policies

About antivirus protection

Symantec Mail Security for Domino detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, Microsoft Word, and Excel files). The outbreak detection feature automatically detects virus outbreaks and sends an alert notification to whomever you designate.

Symantec Mail Security for Domino also includes a decomposer that handles most container, compressed, and archive file formats and nested levels of files, including Zip and RAR. To enhance scanning performance, Symantec Mail Security for Domino contains default settings that limit the depth to which container or compressed files are scanned, but you can modify these settings. You can also limit scanning to certain file types, based on file name extension.

See "Specifying what to scan" on page 84.

Symantec Mail Security for Domino uses the following technologies to protect your system from viruses:

- Bloodhound: Provides heuristic detection of new or unknown viruses
- NAVEX: Provides protection from new classes of viruses automatically through LiveUpdate
- Striker: Detects polymorphic viruses

When a new virus is identified, information about the virus (a virus signature) is stored in a virus definition file. The virus definition file is updated automatically through LiveUpdate. When Symantec Mail Security for Domino scans for viruses, it searches for these virus signatures. To supplement the detection of virus infections by virus signature, Symantec Mail Security for Domino uses Bloodhound technology. Bloodhound technology uses heuristics to detect new or unknown viruses based on the general characteristics that are exhibited by known viruses.

About Bloodhound heuristic technology

Symantec engineers have developed two types of heuristics for the detection of unknown viruses. The first, Bloodhound, is capable of detecting over 80 percent of new and unknown executable file viruses. The second, Bloodhound-Macro, detects and repairs over 90 percent of new and unknown macro viruses.

Bloodhound requires minimal overhead because it examines only programs and documents that meet stringent prerequisites. If Symantec Bloodhound technology identifies suspicious behavior in an executable file, it copies the file into its own virtual computer. It then runs the file and probes for and assesses suspicious behavior, such as whether the file has replicated itself a number of times within a specified period of time. Because the problem file runs within a separate virtual computer that replicates the operating system environment, the potentially infected document cannot harm other documents on the computer.

In most cases, Bloodhound can determine in milliseconds whether a file or document is likely to be infected by a virus. When it determines that a file is not infected, it moves to the next file.

Bloodhound handles executable and macro viruses as follows:

Bloodhound and executable viruses

Bloodhound uses artificial intelligence (AI) technology to isolate and locate the various logical regions of each application that it is configured to scan. It analyzes the program logic in each of these regions for virus-like behavior and simulates this behavior to determine whether the program is a virus.

Bloodhound and macro viruses

Symantec Bloodhound-Macro technology uses a hybrid heuristic scheme to detect and repair more than 90 percent of all new and unknown macro viruses. For example, every time that Symantec Mail Security for Domino scans a Microsoft Word document, Bloodhound-Macro sets up a complete virtual environment into which it loads the document. The macros that are contained in the document are run as they would be in the word processing application.

Bloodhound-Macro monitors the macros as they run to see if they copy themselves from the host document to another virtual document. Bloodhound-Macro also runs the copied macros and verifies whether they can further propagate.

About NAVEX technology

NAVEX is a technology that lets you automatically update the antivirus scanning component of Symantec Mail Security for Domino during routine virus definitions updates. This ensures that your antivirus protection stays current, regardless of platform, against new virus threats without the need for inline revisions or time-consuming upgrades.

The antivirus scanning component is comprised of dozens of complex search algorithms, CPU emulators, and other program logic. The scanning component examines a file to determine if it contains viruses. The scanning component scans files and disks for virus fingerprints (unique sequences of bytes that are known to be contained in viruses). These fingerprints are stored in the virus definition files that are downloaded at least once a week. The scanning component also repairs infected documents.

Occasionally, a new virus or class of virus emerges that cannot be detected by existing scanning components. These viruses require new algorithms for detection and, consequently, a new scanning component. NAVEX technology lets you quickly and efficiently upgrade the Symantec Mail Security for Domino scanning components.

About Striker technology

Striker technology identifies polymorphic computer viruses, which are the most complex and difficult viruses to detect. Like an encrypted virus, a polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer and then decrypts the virus body. A polymorphic virus also adds a mutation engine that generates randomized decryption routines that change each time that a virus infects a new program. As a result, no two polymorphic viruses look alike.

Each time that Striker scans a new program file, it loads the file into a self-contained virtual computer. The program runs in this virtual computer as if it were running on a real computer. The polymorphic virus runs and decrypts itself. Striker then scans, detects, and repairs the virus.

About LiveUpdate

LiveUpdate ensures that your network is not at risk of infection from newly discovered viruses. Updated virus definition files contain the necessary information to detect and eliminate viruses. They are supplied from Symantec at least every week and whenever a new virus threat is discovered. Symantec Mail Security for Domino can be configured to poll the Symantec LiveUpdate servers to determine if updated virus definitions were posted. When new virus definitions are available, Symantec Mail Security for Domino downloads the files and installs them in the proper location. Virus protection stays current without any interruption in protection.

See “Configuring LiveUpdate” on page 181.

Establishing antivirus scanning policies

Customize your antivirus protection by configuring the following settings:

- Basics: Set the Bloodhound heuristic detection level, enable mass-mailer clean up, enable HTML scanning, define the directory for temporary files, and set the memory limits for extracting attachments.
  See “Setting basic antivirus options” on page 105.
- Container Limits: Define the limits for which container files are extracted.
  See “Setting container limits” on page 107.

- Actions: Specify how Symantec Mail Security for Domino should handle infected documents, how to dispose of an infected document that cannot be repaired, whether to repair signed documents, and how to address documents that cannot be scanned.
  See "Defining antivirus action policies" on page 108.
- Outbreak Detection: Establish the criteria and actions for virus outbreaks.
  See "Managing outbreak detection" on page 110.

Setting basic antivirus options

Symantec Mail Security for Domino lets you customize your level of protection against viruses, from zero protection to a high level of protection. A high level of protection increases protection of your system; however, server performance might be affected. At lower levels of protection, the possibility that an unknown virus might escape detection increases, but the trade-off between system performance decreases.

The Bloodhound heuristic virus technology is an advanced heuristic technology that detects a high percentage of new or unknown viruses that have not yet been analyzed by antivirus researchers. Symantec Mail Security for Domino lets you set the resource demand level. In most cases, the default Med (medium) setting is appropriate.

When the mass-mailer cleanup feature is not enabled, an infected mass-mailer email message is treated the same as a virus-infected message. When it is enabled, when Symantec Mail Security for Domino detects that an email message is a mass-mailer worm or virus, it automatically deletes the infected email message and all of its attachments.

To reserve system resources, no antispam or content filtering scan is performed on mass-mailer email messages. Symantec Mail Security for Domino also will not create a backup copy before it deletes the email message or its attachments, even if you have selected this option on the Configuration > Backup tab.

Mass-mailer detection is logged to the specified logging destinations. You can view the Server Status document to determine whether the mass-mailer cleanup feature is enabled, and you can see a count of how many mass-mailer email messages were deleted. The line items in the Server Status document for Files Infected and Files Deleted include mass-mailer email messages along with regular types of viruses. Due to the potential volume of email messages during a mass-mailer outbreak, there is no alerting function for this type of virus detection.

See "Configuring logging options" on page 88.

See "Checking server status" on page 51.

Multipurpose Internet Mail Extensions (MIME) is the official Internet standard for encoding data that cannot be transmitted through email. Symantec Mail Security for Domino lets you scan email messages for malicious code in native MIME message bodies.

Symantec Mail Security for Domino uses the default Windows TEMP directory to process files during scans. If necessary, you can specify a directory on another drive that has more space available. You must have at least 100 MB of free space on the drive that contains this directory. If you type a directory that is not valid, Symantec Mail Security for Domino uses the Windows TEMP directory. If you are using a third-party antivirus product (not a Symantec product) with Symantec Mail Security for Domino, you should configure the third-party product not to scan this directory. This prevents potential conflicts with Symantec Mail Security for Domino operation.

To set basic antivirus options

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antivirus tab, on the Basic tab, under Bloodhound heuristic virus detection technology, select the appropriate level of detection.
   The default setting is Med (medium).
3. To automatically delete infected mass-mailer email messages and their attachments, under Mass-Mailer Cleanup, click **On**.
   This option is enabled by default.
4. To scan native MIME message bodies, under Scan Native MIME message bodies, click **On**.
5. If you want to use a directory other than the Windows TEMP directory, under Directory for temporary files, type the new directory location.
   If you are using a third-party antivirus product, configure the third-party product not to scan this directory. This prevents conflicts with Symantec Mail Security for Domino operations.
6. To limit the RAM used to examine files in memory, under Maximum memory to use per thread for extracting attachments, type the appropriate number of kilobytes.
   The default setting is 20000.
7. On the Action bar, click **Save**.

Setting container limits

Symantec Mail Security for Domino contains a decomposer that extracts container files so that they can be scanned for viruses. The decomposer continues to extract container files until it reaches the base file.

Symantec Mail Security for Domino imposes limits on file extraction. These limits protect against denial-of-service attacks that are associated with overly large or complex container files that take a long time to decompose. These limits also enhance scanning performance. When a container file reaches any one of the set limits, the scanning process stops, a scan error violation is logged to the specified logging destinations, and the file is disposed of according to the antivirus action policies.

See "Defining antivirus action policies" on page 108.

The default values are the minimum values. Symantec Mail Security for Domino does not accept any values that are less than the minimum values. The maximum values are limited by 32-bit data size. If you type an incorrect value, you receive an error message that indicates the allowable minimum and maximum values.

Warning: The maximum values for container limits are based on operating system and hardware limitations. Increasing the container limit values without full knowledge of your specific system limitations could result in a system failure. If you are uncertain about how an increase to the values might affect your Domino server, you should maintain the default, minimum values.

To set container limits

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antivirus tab, on the Container Limits tab, under Messages that exceed any set container limit will be reported as scan errors, modify any of following:
   - Attachment that takes more than 300 seconds to extract.
   - Attachment that contains more than 10 levels of nested containers.
   - Attachment where any one file extracts to more than 50 MBs in size.
   - Attachment where the cumulative size of all extracted files exceeds 200 MBs.
   - Attachment where the number of files extracted exceeds 5000.
3. On the Action bar, click **Save**.

Defining antivirus action policies

Action policies define which action Symantec Mail Security for Domino takes when a virus is detected or when a document is unable to be scanned. Unscannable documents might include encrypted container files or files that result in a scan error.

If you choose the option to Delete the infected attachment, Symantec Mail Security for Domino saves the deleted attachment as a backup document in the Quarantine. When Symantec Mail Security for Domino detects a virus inside a container file, it deletes the container file and everything in it. When a container file is comprised of both infected and uninfected files, the entire container file and all the files inside it might be deleted.

Symantec Mail Security for Domino scans ID-signed documents for viruses, but it must break the signature to repair an infected document. When the Repair signed documents option is enabled, Symantec Mail Security for Domino breaks the signature and attempts to repair the document.

When the Repair signed document option is not enabled and Symantec Mail Security for Domino detects a virus in an ID-signed document, it treats the document as unrepairable. If this option is not enabled and you selected the Repair the infected attachment option on any of the scan tabs (Auto-Protect, Scan Now, or Scheduled Scans), Symantec Mail Security for Domino handles the ID-signed document according to the configuration settings on the Scan tab.

Note: Symantec Mail Security for Domino attempts to repair ID-signed documents, but not X.509 Certificate-signed documents.

To define antivirus action policies

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antivirus tab, on the Actions tab, under When a virus is detected, select one of the following:

Log only	Logs the detection but takes no action.
Delete the infected attachment	Deletes the infected attachment. Deleted attachments are not recoverable. Symantec Mail Security for Domino adds explanatory text to the attachment icon.

Quarantine the document	Holds the infected document in the Quarantine database for administrator review. You must have the appropriate Role assignments to view quarantined documents. See "Managing quarantined documents" on page 214. See "Assigning Quarantine roles" on page 216.
Repair the infected attachment	Automatically deletes the virus and repairs any damage. This option is enabled by default. If Symantec Mail Security for Domino cannot repair the document, the selected If unable to repair option applies.

3. If you select Repair the infected attachment, under If unable to repair, select one of the following options for disposing of unrepairable infected documents:
   - Log only
   - Delete the infected attachment
   - Quarantine the document
     This option is enabled by default.
4. To eliminate viruses from ID-signed documents, under Repair signed documents, click **Yes**.
   This option is enabled by default.
5. To dispose of an encrypted container file that cannot be scanned, under When messages are unable to be scanned Due to encrypted containers, select one of the following:
   - Log only
     This option is enabled by default.
   - Delete the attachment
   - Quarantine the document
6. To dispose of the scan error file, under Due to scan errors, select one of the following:
   - Log only
   - Delete the attachment
   - Quarantine the document
     This option is enabled by default.
7. On the Action bar, click **Save**.

Managing outbreak detection

A virus outbreak is suspected when Symantec Mail Security for Domino detects an excessive number of viruses or events that exhibit virus-like behavior on Domino servers. When Symantec Mail Security for Domino suspects a virus outbreak, prompt action is necessary. The outbreak management feature lets you protect systems during an outbreak, even before you receive the latest virus definitions.

Symantec Mail Security for Domino helps you manage virus outbreaks as follows:

- Specify the criteria for an outbreak.

  These criteria consist of the detection method to use (basic or advanced) and the number of times that suspicious incidents must occur over a specified time to qualify as an outbreak.

  The basic detection method tallies all of the viruses that are detected. The advanced detection method only tallies viruses that have the same characteristics. For example, given a threshold of 10 viruses in 10 minutes, a count of nine KakWorm infections and nine Nimda infections would cause the basic option to trigger an outbreak, but not the advanced option. However, a count of 10 KakWorm and two Nimda infections would cause both the basic and advanced options to trigger an outbreak.
- Define who to notify when the criteria for a virus outbreak are met.

  The outbreak management settings in Symantec Mail Security for Domino are enabled by default. Symantec Mail Security for Domino is configured to report an outbreak incident in the Symantec Mail Security for Domino Log when it detects more than 30 viruses of any type within 10 minutes. You must specify who to alert when an outbreak occurs.

You can change the number of virus detections that are necessary to trigger an outbreak notification and the time span in which the possible infections are detected. There are no set guidelines to use when specifying frequencies, so take into account the threat potential of the type of documents that are being monitored, the size of your email system, the amount of mail that is typically processed, and the stringency with which you want to define an outbreak.

As your outbreak settings are tested, you can fine-tune the values that you use. Symantec Mail Security for Domino logs virus detections and (possibly) sends alerts when it detects an outbreak, so your goal is to strike a balance between catching outbreaks and issuing unnecessary notifications.

To manage outbreak detection

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antivirus tab, on the Outbreak Detection tab, check **Enable virus outbreak detection**.
   This option is enabled by default.
3. Under Detection Type, select one of the following:
   - Basic (Add all viruses to virus count)
     This option is enabled by default.
   - Advanced (Add only viruses with similarities to virus count)
4. Under Threshold and Notification, do any of the following:
   - Type the number of viruses to be detected within the specified time frame.
     The default setting is 30.
   - Type the specified time frame (in minutes) in which the number of detected viruses is considered an outbreak.
     The default setting is 10.
   - In the drop-down list, select the names of those to whom email notifications should be sent.
5. On the Action bar, click **Save**.

Chapter 7

Filtering unwanted content

This chapter includes the following topics:

About content filtering

Symantec Mail Security for Domino enhances mail security protection by blocking email messages and documents based on content. You can search the subject lines or contents of email messages and their attachments for offensive language, confidential information, and content with potential legal consequences.

To search for unwanted content, you create content filtering rules. When the content or some attribute of a document or email message violates a rule, Symantec Mail Security for Domino disposes of the document based on the settings that you configure for that rule.

You can set up as many content filtering rules as you need. Each rule specifies the category to search and defines the condition that triggers a content filtering rule violation.

See "Creating a content filtering rule" on page 118.

Content filtering is typically used to monitor the mail system and block messages that contain specific types of content. For example, in most organizations, sending messages with explicit sexual or violent content is not an appropriate use of the company mail system and violates corporate conduct guidelines. In other cases, an organization might want to prevent the spread of confidential information outside of the organization or block messages that could have adverse legal consequences for the organization.

How Symantec Mail Security for Domino filters content

Symantec Mail Security for Domino filters unwanted content by using a Dynamic Document Review (DDR). The DDR is a multilingual, context-sensitive content analysis technology that evaluates documents against scoring thresholds that you define. When documents exceed the scores, Symantec Mail Security for Domino handles the document according to the settings that you configure.

Symantec Mail Security for Domino lets you create content filtering rules to apply to Notes document writes and incoming email messages. The rules provide a front-end defense against unwanted content for a server group. These rules expand the control that administrators have to block objectionable email messages and other documents that are created in Lotus Notes databases.

You can set up, edit, or delete as many content filtering rules as you need. Each rule specifies the category to search (subject line, sender, or file size, for example), and defines the condition that triggers a content filtering rule violation. You can enable or disable the content filtering process or individual rules.

See “Creating a content filtering rule” on page 118.

You can create match lists and custom word categories, and then use them in content filtering rules. Match lists let you create a list of words and phrases that are tailored to your company or industry. You can then create a content filtering rule to evaluate content for words in your match list.

See “Using a match list” on page 133.

Symantec Mail Security for Domino comes with a dictionary of commonly filtered words and phrases, which is organized into categories. You can use these word categories in content filtering rules, or you can create your own custom word category.

A custom word category is a user-customized repository of inappropriate words and phrases. Each word and phrase is assigned a score, which is added to the overall content score. Custom word categories let you determine the relative weight that is assigned to a word or phrase when you use content scoring in a content filtering rule.

See "Filtering content with word categories" on page 136.

Working with content filtering rules

Table 7-1 lists the ways in which you can work with content filtering rules.

Table 7-1 Content filtering rule tasks

Task	Description
View the status of content filtering rules.	Symantec Mail Security for Domino lets you view all of the default content filtering rules as well as the rules that you have created. You can view whether the rule is enabled. You can also view a description of the content filtering rule and for which type of scan the rule applies. See "Viewing the status of content filtering rules" on page 116.
Enable the content filtering rule process.	To activate content filtering for any type of scanning, you must enable the rules processing option. See "Enabling the content filtering process" on page 116.
Enable default content filtering rules.	Select the pre-configured content filtering rules that you want to use. See "Enabling default content filtering rules" on page 117.
Create a new content filtering rule.	Create your own content filtering rule to block sensitive or objectionable content. See "Creating a content filtering rule" on page 118.
Delete a content filtering rule.	Delete a content filtering rule that you no longer need. See "Deleting a content filtering rule" on page 133.

Viewing the status of content filtering rules

Symantec Mail Security for Domino displays the status of default content filtering rules, and any new rules that you have created, on the Content Filtering > Rules tab.

The list of rules shows whether the rule is enabled and the type of content or scan for which the rule is configured. A green check mark indicates that the option is enabled for the rule. A red X indicates that the option is not enabled.

The type of content or scans for which a content filtering rule can be applied are as follows:

- Email messages
- Writes (documents saved to the server)
- Scheduled scans
- Scan now scans

In addition, you can view whether the Stop option is enabled for each rule. The Stop option stops processing the content filtering rule after Symantec Mail Security for Domino detects the first violation.

To view content filtering rules status

1. In the Settings view, double-click a server group.
2. In the Group document, on the Content Filtering tab, click the **Rules** tab to display the list of content filtering rules and their statuses.

Enabling the content filtering process

To configure Symantec Mail Security for Domino to perform content filtering, you must enable rules processing. During a content filtering scan, Symantec Mail Security for Domino applies only the content filtering rules that are enabled. You must also enable the individual content filtering rules that you want to use during the scanning process.

See “Setting the basic options for a content filtering rule” on page 119.

To enable the content filtering process

1. In the Group document, on the Content Filtering tab, on the Rules tab, check **Enable rules processing**.
2. On the Action bar, click **Save**.

Enabling default content filtering rules

Symantec Mail Security for Domino has several default content filtering rules that are preconfigured for you. Default content filtering rules are part of the Unassigned Servers settings. To use any of these rules, you must copy the Unassigned Server settings to a new server group, which you must create. You can disable or delete any rules that are no longer needed.

See "Copying settings to create a new server group" on page 81.

As an alternative, you can view the default content filtering rule settings, and then recreate the rule for another server group.

The following default rules are available:

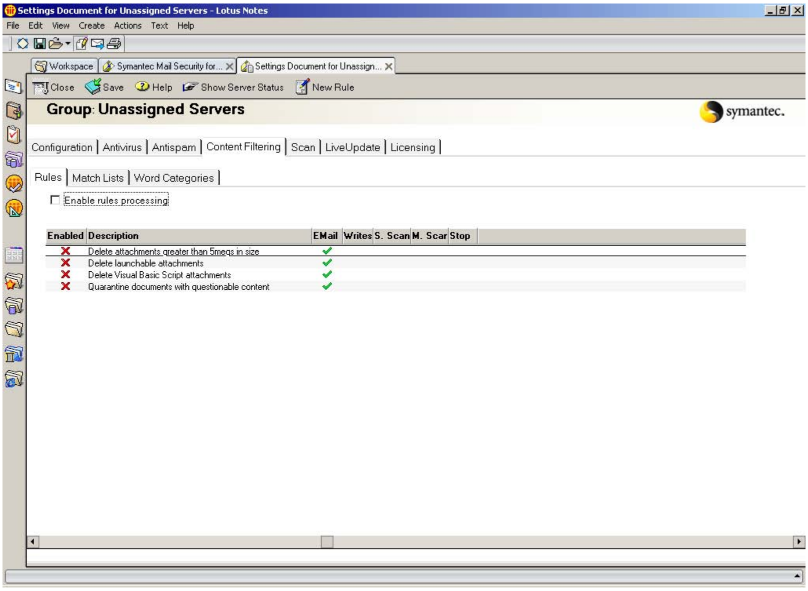
- Delete attachments greater than 5megs in size
- Delete launchable attachments
- Delete Visual Basic Script attachments
- Quarantine documents with questionable content

Content filtering is turned off by default. To scan for content filtering rule violations, you must enable rules processing in addition to enabling each rule that you want to use.

See "Enabling the content filtering process" on page 116.

To enable default content filtering rules

1 In the Group document, on the Content Filtering tab, on the Rules tab, double-click the rule that you want to enable.



Group: Unassigned Servers

☐ Enable rules processing

Enabled	Description	EMail	Writes	S. Scan	M. Scar	Stop
✗	Delete attachments greater than 5megs in size	✓				
✗	Delete launchable attachments	✓				
✗	Delete Visual Basic Script attachments	✓				
✗	Quarantine documents with questionable content	✓				

2 In the Content Filtering Rule document, on the Basics tab, check **Enable this rule**.

3 On the Action bar, click **Save**.

Creating a content filtering rule

To create a content filtering rule, you specify the basic settings and set up as many conditional expressions as you need to categorize the objectionable content that you are trying to block. You can then specify how to handle a document that violates the content filtering rule.

To create a content filtering rule

1 In the Group document, on the Content Filtering tab, on the Rules tab, on the Action bar, click **New Rule**.

2 In the Content Filtering Rule document, on the Basics tab, set the basic options.
See “Setting the basic options for a content filtering rule” on page 119.

3 On the Rule tab, use expressions to define the content filtering rule.
See "Working with content filtering rule expressions" on page 120.
See "Building expressions for a content filtering rule" on page 128.

4 On the Actions tab, set the action options.
See "Setting the action options for a content filtering rule" on page 132.

5 On the Action bar, click **Save**.

6 On the Action bar, click **Close** to return to the Content Filtering tab.
When you are ready to process the rule, ensure that it is enabled on the Basics tab. In addition, ensure that rules processing is enabled on the Content Filtering > Rules tab.
See "Enabling the content filtering process" on page 116.

Setting the basic options for a content filtering rule

When setting up a content filtering rule, you must enable the rule and set up the basic options.

Warning: Applying most content filtering rules to Domino databases will cause severe data loss and may destabilize servers.

To set the basic options for a content filtering rule

1 In the Content Filtering Rule document, on the Basics tab, check **Enable this Rule.**
This option is enabled by default.

2 Under Description, type a description for the content filtering rule.
Provide a meaningful name for the content filtering rule so that you can identify it in the content filtering rules status and in the Symantec Mail Security for Domino Log.

3 Under This rule is for, select any of the following:

Email routing	Applies the content filtering rule to email messages. This option is enabled by default.
Document writes	Applies the content filtering rule to documents that are saved to the Lotus Domino databases (not recommended).
Scheduled Scans	Applies the content filtering rule to scheduled scans. You must also enable the option to scan for content filtering rule violations on the Scheduled Scan > What to Scan tab.
Manual Scans	Applies the content filtering rule to scan now scans. You must also enable the option to scan for content filtering rule violations on the Scan Now > What to Scan tab.

4 Under Servers, This rule is valid for, select one of the following:

- All servers in this group: Applies the rule to all servers in the server group.
  This option is enabled by default.
- The following servers: Applies the rule to the servers that you select. In the drop-down list, select the servers for which this rule applies.
  Use commas to separate multiple servers.

5 On the Action bar, click **Save**.

Working with content filtering rule expressions

A content filtering rule consists of one or more expressions that you define. For example, the following content filtering rule contains three expressions:

If Content Score > [50] using categories [sex;drugs;alcoholism]
OR Content Score > [90] using categories [politics]
UNLESS Sender = [Fred Smith/WestRegion/AcmeInc]

An expression consists of one or more expression phrases. Expression phrases can be IF, OR, AND, or UNLESS phrases. The rule in the example consists of an IF, an OR, and an UNLESS phrase.

Symantec Mail Security for Domino evaluates a rule logically as either an OR or AND rule, but not in combination. You can have a rule that contains an IF phrase, any number of AND phrases, and any number of UNLESS phrases, but it cannot contain an OR phrase when it already has an AND phrase. Likewise, when you start with an OR phrase, you can add more OR phrases or UNLESS phrases, but not an AND phrase.

An expression phrase consists of the following elements:

Attribute

The part or characteristic of the email message or document that you want to scrutinize for violations.

Attributes include Sender/Author, Subject, Body, Size (of entire email message or document, in bytes), Encryption Flag (true or false), Internet Domain, Domino Server, Domino Domain, Attachment name, Attachment extension, Attachment size (in bytes), and Content Score.

Comparison

The comparison that you want to make between the attribute and the value that, when matched to the attribute, constitutes a content filtering rule violation.

Operators include Contains, Does not contain, = (equals), <> (does not equal), > (greater than), and < (less than). The availability of certain operators is limited by the attribute that is selected.

Value

The numeric value or alphanumeric text string that you type as the criteria to match.

The attributes of Size, Attachment size, and Content Score are numeric values. The Encryption Flag Attribute is a Boolean True or False value, while the rest are alphanumeric text strings.

When you select Item(s) from Match List, one or more match lists display, if you have created any. You then select a match list as the criteria to match.

See “Creating a content filtering rule that uses a match list” on page 136.

The attribute that you select determines which operators that you can use. Some attributes have more operators than others. For example, if you select Sender/Author as the attribute, then the available operators are Contains, Does not contain, =, and <>. However, if you choose Encryption Flag as the attribute, then only the = operator is available.

Most attributes (Attachment name, Attachment ext., Body, Domino Domain, Domino Server, Internet Domain, Sender/Author, and Subject) take alphanumeric text strings as their values. This means that even if you type a number in the Value box, Symantec Mail Security for Domino considers it text, not a number. Because they allow for regular expressions, text strings give you flexibility in extending your text searches to find more than just a direct match. Regular expressions include metacharacters, or wildcard characters, to help you broaden the search capabilities of a given rule.

See “About regular expressions” on page 122.

Selecting Content Score as the attribute instructs Symantec Mail Security for Domino to use Dynamic Document Review to analyze the content based on a score and one or more dictionary content categories that you specify for that rule. Symantec Mail Security for Domino considers any document with a score that exceeds your specified threshold value to be a content filtering rule violation, and it takes the action that you have specified for the rule. The threshold for a content filtering rule violation might be a single word, phrase, or name, which might appear in the subject line or body of a message, or it might be multiple occurrences, as determined by the content score engine.

See “Filtering content with word categories” on page 136.

About regular expressions

A regular expression is a set of symbols and syntactic elements that is used to match patterns of text. Symantec Mail Security for Domino performs matching on a line-by-line basis. It does not evaluate the line feed (newline) character at the end of each input expression phrase.

You can build regular expressions using a combination of normal alphanumeric characters and metacharacters, also called wildcard characters. Metacharacters let you perform pattern matching in text. For example, many spam messages contain a trailing number at the end of the subject line text, as in the following sample subject line:

Here’s a hot stock pick!43234

An example of how to write a rule to detect email message subject lines that have trailing numbers using regular expressions is as follows:

ˆ.*[0-9]$

This regular expression contains the normal alphanumeric characters 0-9 and the metacharacters ˆ, ., *, and []. By using the Subject attribute, the = operator, and the regular expression as the value, you can build a content filtering rule to catch any email message whose subject line ends with a trailing number, a probable sign that the message is spam.

See “About metacharacters” on page 123.

As another example, you might want to filter email message attachments with certain file name extensions. To detect message attachments with the file name extensions .exe, .com, or .zip, you could write three different expression phrases, each focusing on one of the extensions. A more practical and faster way to do it is to use the pipe metacharacter (|), which creates an OR expression, for example:

Attachment ext. = com|exe|zip

This example matches any first-level extension name that equals .com, .exe, or .zip.

Note: For content filtering only, first-level attachments refer to the outer-most file attachment. The content filtering engine does not evaluate any file name extension inside the outer attachment, for example, the compressed files in a .zip file.

About metacharacters

Table 7-2 lists the metacharacters that you can use in regular expressions to build content filtering rules. Some characters are not considered special unless you use them in combination with other characters.

Note: You can use metacharacters in regular expressions to search for both single-byte and multi-byte character patterns.

Table 7-2 Metacharacters for regular expressions

Metacharacter	Meaning
.	Period: Matches any single character of the input sequence.
ˆ	Circumflex: Represents the beginning of the input line. For example, ˆA is a regular expression that matches the letter A at the beginning of a line. The ˆ character is only special at the beginning of a regular expression or after the (or | characters.
$	Dollar sign: Represents the end of the input line. For example, A$ is a regular expression that matches the letter A at the end of a line. The $ character is only special at the end of a regular expression or before the) or | characters.

Table 7-2 Metacharacters for regular expressions

Metacharacter	Meaning
*	Asterisk: Matches zero or more instances of the string to the immediate left of the asterisk. For example, A* matches A, AA, AAA, and so on. It also matches the null string (zero occurrences of A).
?	Question mark: Matches zero or one instance of the character to the immediate left of the question mark.
+	Plus sign: Matches one or more instances of the string to the immediate left of the plus sign.
\	Escape: Turns on or off the special meaning of metacharacters. For example, \. only matches a dot character. \$ matches a literal dollar sign character. Note that \\ matches a literal \ character.
|	Pipe: Matches either expression on either side of the pipe. For example, exe|com|zip matches exe, com, or zip.
[string]	Brackets: Inside the brackets, matches a single character or collating element, as in a list. The string inside the brackets is evaluated literally, as if an escape character (\) were placed before each character in the string. If the initial character in the brackets is a circumflex (ˆ), then the expression matches any character or collating element except those inside the bracket expression. Specify character ranges with a hyphen (-) between two characters or collating sequences to indicate the range of all characters or collating sequences between the explicit ones on either side of the hyphen. The range does not refer to the native character set. For example, in the POSIX locale, [a-z] means all lowercase letters even when they do not agree with the binary machine ordering. However, because many other locales do not collate in this manner, avoid ranges in strictly conforming POSIX.2 applications. A collating sequence might explicitly be an endpoint of a range. For example, [[.ch.]-[.11.]] is valid; however, equivalence or character classes might not be valid. For example, [[=a=]-z] is illegal. If the first character after any potential circumflex (ˆ) is a hyphen (-) or a closing bracket (]), then that character matches only a literal dash or closing bracket.

Table 7-2 Metacharacters for regular expressions

Metacharacter	Meaning
char{n} char\{n\}	A single character (char) followed by a number (n) in braces: Matches the number of repetitions of the character. For example, X\{3\} matches XXX.
char{min,} char\{min,\}	A single character (char) followed by a number (min) and a comma in braces: Matches the minimum number of repetitions of the character. For example, X\{3,\} matches at least three repetitions of X.
char{min,max} char\{min, max\}	A single character (char) followed by a pair of numbers in braces: Matches the minimum number of repetitions of the character, but no more than the maximum number of repetitions. For example, X\{3,7\} matches from three to seven repetitions of X.
(string) \(string\)	Parentheses: Groups parts of regular expressions, giving the string inside the parentheses precedence over the rest.
\<	Backslash followed by a less than sign: Matches the beginning of an identifier, defined as the boundary between nonalphanumeric and alphanumeric characters, including the underscore character (_). This expression matches no characters, only the context.
\>	Backslash followed by a greater than sign: Matches the end of an identifier, defined as the boundary between nonalphanumeric and alphanumeric characters, including the underscore character (_). This expression matches no characters, only the context.

When multiple metacharacters are used in an expression, Symantec Mail Security for Domino evaluates certain metacharacters before others.

Table 7-3 lists the order in which Symantec Mail Security for Domino evaluates metacharacters, from highest to lowest precedence.

Table 7-3 Metacharacter order

Metacharacter	Meaning
()	Precedence override
|	OR

Table 7-3 Metacharacter order

Metacharacter	Meaning
[]	List
\	Escape
ˆ	Start with

Examples of regular expressions that filter email messages

You can link several regular expressions to form a larger one to match certain content in email messages.

Table 7-4 provides examples of regular expressions that show how pattern matching is accomplished through the use of metacharacters and alphanumeric characters.

Table 7-4 Examples of regular expressions that filter email messages

Regular expression	Meaning
abc	Matches any line of text that contains the three letters abc in that order. Your results might differ depending on the comparison operator that you use to create the content filtering rule. For example, if you build a rule to match the word “free” and use the Contains comparison, then the content filtering engine detects all words that contain the word free instead of an exact match (for example, Freedom). However, if you use the = (equal) comparison, then the content filtering engine detects only exact matches of the word Free.
a.c	Matches any string that begins with the letter a, followed by any character, followed by the letter c.
ˆ.$	Matches any line that contains exactly one character. The newline character is not counted.
a(b*|c*)d	Matches any string that begins with the letter a, followed by either zero or more instances of the letter b, or zero or more instances of the letter c, followed by the letter d.

Table 7-4 Examples of regular expressions that filter email messages

Regular expression	Meaning
.* [a-z]+ .*	Matches any line that contains a word that consists of lowercase alphabetic characters, delimited by at least one space on each side.
(text).*\1 text.*text	Both expressions match lines that contain at least two occurrences of the string text.
[[:space:][:alnum:]]	Matches any character that is either a whitespace character or alphanumeric.
.+\....\....	Matches any file name that has two, three-letter extensions (for example, Filename.gif.exe). This regular expression is helpful in blocking email message attachments with double extensions. For example: If Attachment Name = .+\....\....
.+Part Number:([[:upper:]])\1[[:number:]]+	Matches a sentence such as: "...included is a description of Part Number:ZZ487584 and we have it in stock." Note that the first two characters of the part number are uppercase and are the same character.
[0-9a-zA-Z]+<!--.*-->[0-9a-zA-Z]+	Matches an embedded comment in the middle of meaningful HTML text. Embedding comments within HTML text is a trick that spam senders use to bypass most pattern-matching software.

Table 7-4 Examples of regular expressions that filter email messages

Regular expression	Meaning
ˆ.+\ +[0-9]+$	Matches a subject in an email message that might look like the following: "Earn big money today 434323" Note that the metacharacters ˆ and $ mark the beginning and end of the line. These characters are optional, depending on whether you use the comparison Contains or = (equals). When you create your content filtering rule using =, the content filtering engine automatically surrounds the regular expression with these two metacharacters to find an exact match. When you use Contains, the two metacharacters are not included.

Building expressions for a content filtering rule

Table 7-5 lists the expression options for a content filtering rule.

Table 7-5 Content filtering expression options

Expression	Meaning
If	Sets up the expression to be a condition of the content filtering rule. The first expression that you create must consist of an IF expression.
Unless	Sets up the expression to be an exception to all conditional (IF) expressions.
Attribute	Selects the basis for the rule. For example, if you select Sender as the attribute, the content filtering rule only applies to documents or email messages that are created by the sender that you specify.

Table 7-5 Content filtering expression options

Expression	Meaning
Comparison	Selects the relationship between the attribute and the value. Available comparison options change depending on the attribute that you select. For example, if you select Size as the attribute, the available comparison options are > (greater than), < (less than), = (equal to), and <> (not equal to). Other attributes might yield different sets of options. When you select the Body attribute, along with the comparison options, you also see an option to ignore the case, which lets you specify a value in any combination of uppercase or lowercase letters.
Value	Specifies the word, phrase, or numerical quantity that limits the attribute of the rule in one way or the other, as defined by the selected comparison (relationship). The type of attribute that is selected dictates the type of value that you enter. For example, if you select the Size attribute, you must type a number as the value. When you type file name extensions, omit the dot (.) before the extension. Values can include single-byte or multi-byte characters. When you select Content Score as the Attribute, in the value box, Symantec Mail Security for Domino provides the list of word categories from which you can select. You must also type the numerical value for the comparison with the Content Score. See "Creating a content filtering rule that uses word categories" on page 144. When you select Item(s) from match list, all match lists that have been created appear. You then select the match list that you want to filter content against. See "Creating a content filtering rule that uses a match list" on page 136.
AND/OR	Appends an AND or OR conjunction to the expression, which sets up its relationship to the next expression. Final or single expressions do not require a conjunction. When building multiple expressions in a rule, you must use all AND or all OR expressions. AND and OR conjunctions cannot be mixed in the same rule.
Add	Adds the expression to the List of Expressions.

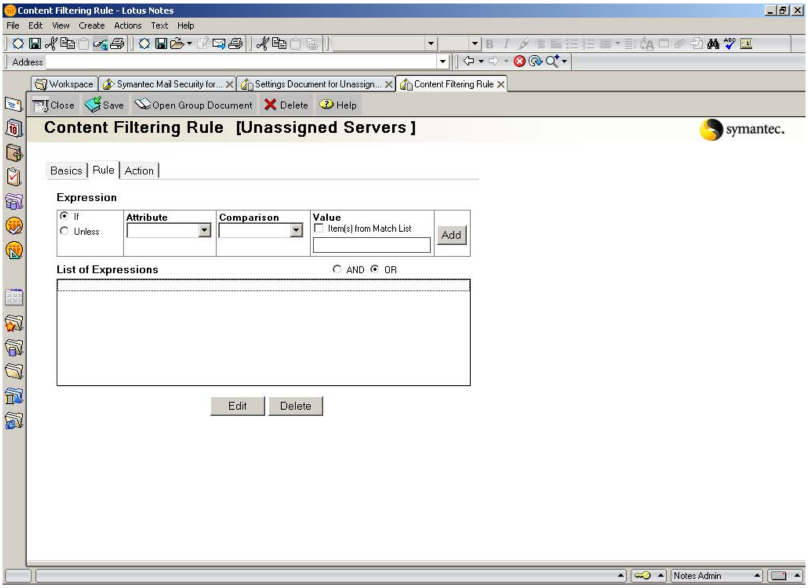
Table 7-5 Content filtering expression options

Expression	Meaning
List of Expressions	Lists all of the expressions that you have created for the content filtering rule that you are configuring.
Edit	Redisplays the selected expression in the List of Expressions so that you can modify the elements of the expression as necessary.
Delete	Deletes the expression that is selected in the List of Expressions.

You can define and add multiple content filtering rule conditions and edit or delete expressions. Your first expression must be an If statement.

To create an expression for a content filtering rule

1 In the Content Filtering Rule document, on the Rule tab, under Expression, ensure If is selected.
This option is enabled by default.



Content Filtering Rule [Unassigned Servers]

● If
○ Unless

□ Item(s) from Match List

○ AND ● OR

2 Under Attribute, in the drop-down list, select the appropriate attribute.

3 Under Comparison, in the drop-down list, select the appropriate comparison option.
Comparison options change depending on the attribute that you select.

4 Under Value, type the threshold value.
Value options change depending on the attribute that you select.

5 Click **Add**.

6 On the Action bar, click **Save**.

To add multiple expressions to a content filtering rule

1 After you define the first content filtering rule expression, in the Content Filtering Rule document, on the Rule tab, click **AND** or **OR** to create a rule with multiple expressions.
When building multiple expressions in a rule, you must use all AND or all OR expressions. AND and OR conjunctions cannot be used in the same rule.

2 Under Expression, select one of the following:

- If
- Unless

3 Under Attribute, in the drop-down list, select the appropriate attribute.

4 Under Comparison, in the drop-down list, select the appropriate comparison option.
Comparison options change depending on the attribute that you select.

5 Under Value, type the threshold value.
Value options change depending on the attribute that you select.

6 Click **Add**.

7 On the Action bar, click **Save**.

To edit an expression

1 Under List of Expressions, select the expression that you want to edit.

2 Click **Edit**.

3 Modify any of the expression options.

4 To the right of the Value box, click **Save**.

5 On the Action bar, click **Save**.

To delete an expression

1 Under List of Expressions, select the expression that you want to delete.

2 Click **Delete**.

3 On the Action bar, click **Save**.

Setting the action options for a content filtering rule

You must configure how to dispose of documents that contain content filtering rule violations.

You can configure Symantec Mail Security for Domino to stop evaluating the document for additional content filtering rule violations after the first content filtering rule violation is found. This helps optimize performance.

To set the action options for a content filtering rule

1 In the Content Filtering Rule Document, on the Action tab, under When a violation is detected, select one of the following:

Log only	Logs the violation only but does nothing with the document. This option is enabled by default.
Delete the attachment(s) which meet the criteria	Deletes only the attachment that has a name, extension, content, or size that violates a content filtering rule.
Delete all attachments	Deletes all of the attachments, even if the violation is detected only in the email message text.
Quarantine the document	Holds the document in the Quarantine database for administrator review. To view or take action on quarantined documents, you must have the appropriate role privileges. See "Managing quarantined documents" on page 214.
Copy the document to the Quarantine database	Creates a backup copy of the document that contains the content filtering rule violation and places it in the Backup Documents view of the Symantec Mail Security for Domino Log.
Delete the document	Deletes the document that triggered the content filtering rule violation.

2 To stop the content filtering engine from evaluating the document for additional content filtering rule violations after the first violation is detected, click **Stop processing more rules**.

3 On the Action bar, click **Save**.

Deleting a content filtering rule

When you no longer need a content filtering rule, you can delete it from the content filtering rules list.

To delete a content filtering rule

1. In the Group document, on the Content Filtering tab, on the Rules tab, double-click the rule that you want to delete.
2. In the Content Filtering Rule document, on the Action bar, click **Delete**.
3. In the SMSDOM Settings dialog box, click **Yes** to confirm that you want to delete the content filtering rule.
4. On the Action bar, click **Save**.

Using a match list

Match lists let you create a custom list of words and phrases that are standard for or particular to your company or industry, and for which you want to filter content. After you develop a match list, you can create a content filtering rule that uses words and phrases in the match list.

How a match list works

When you use a match list in a content filtering rule, you typically select a comparison value of either Contains or = (equals). These values operate differently on words in a match list. Use the = value to detect exact matches for words. Use the Contains value to detect words that contain the letters. Match list names are case-sensitive. Words and phrases within the match list are not case-sensitive.

For example, if the word Free is included in the match list, a content filtering rule violation occurs only when the document contains an exact match of the word Free. However, if the word Free is in your match list and you select Contains as your comparison value, then a content filtering rule violation occurs whenever the content filtering rule finds the letters Free (for example, as in Freedom).

Building a match list

When you create a match list, give it a name that best describes the category of words and phrases that you intend to include in the list. You can create as many match lists as you need.

After you create a match list, you can create a content filtering rule that uses the match list. The criteria for the content filtering rule applies to any word or phrase that is in the match list.

A match list contains the words and phrases that you assign to it. You can add, edit, or delete words or phrases in a match list. A match list must contain at least one word or phrase.

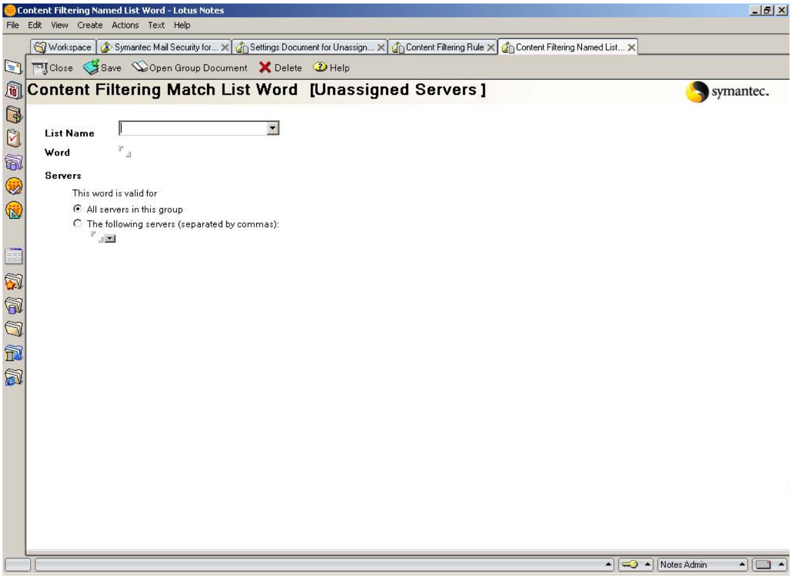
You can compose words in English or in single-byte or multi-byte international characters. The content filtering engine treats the word or phrase that you type as a regular expression. This means that you must use the escape character (\) to turn off the special meaning of any metacharacters that you include in the word or phrase.

See “About metacharacters” on page 123.

To add a word or phrase to a match list

1 In the Group document, on the Content Filtering tab, click the **Match Lists** tab.

2 On the Action bar, click **New Word in Match List**.


Content Filtering Named List Word - Lotus Notes
File
Edit
View
Create
Actions
Text
Help
Workspace
Symantec Mail Security for...
Settings Document for Unassign...
Content Filtering Rule
Content Filtering Named List...
Close
Save
Open Group Document
Delete
Help
symantec.
Notes Admin

Content Filtering Match List Word [Unassigned Servers]

List Name

Word

Servers

This word is valid for

● All servers in this group

○ The following servers (separated by commas):

3 In the Content Filtering Match List Word document, in the List Name box, do one of the following:

- If you are creating a new match list, type a name for the match list.
  Match list names are case-sensitive.
- If you have already created a list and want to assign the new word or phrase to the existing match list, in the drop-down list, select the match list name.

4 In the Word box, type a custom word or phrase to add to the match list.
Words in the match list are not case-sensitive.

5 Under Servers, select one of the following:

- All servers in this group: Applies the word or phrase to all servers in the server group
  This option is enabled by default.
- The following servers: Applies the word or phrase to specific servers Select the servers from the drop-down list. Separate multiple entries with commas.

6 On the Action bar, click **Save**.

To edit a word or phrase in a match list

1 In the Group document, on the Content Filtering tab, on the Match Lists tab, under Word/Phrase, double-click the word or phrase that you want to edit.

2 In the Content Filtering Match List Word document, make revisions as necessary.

3 On the Action bar, click **Save**.

To delete a word or phrase in a match list

1 In the Group document, on the Content Filtering tab, on the Match Lists tab, under Word/Phrase, double-click the word or phrase that you want to delete.

2 In the Content Filtering Match List Word document, on the Action bar, click **Delete**.

3 In the confirmation dialog box, click **Yes**.

4 On the Action bar, click **Save**.
Symantec Mail Security for Domino automatically deletes a match list when all of the words or phrases within the match list are deleted.

Creating a content filtering rule that uses a match list

After you have built your match list, you can create content filtering rules that use the match list.

To create a content filtering rule that uses a match list

1. In the Group document, on the Content Filtering tab, click the **Rules** tab.
2. On the Action bar, click **New Rule**.
3. In the Content Filtering Rule document, on the Basics tab, set the basic options.
   See "Setting the basic options for a content filtering rule" on page 119.
4. On the Rule tab, set the If attribute, and then select comparison options.
   See "Creating a content filtering rule" on page 118.
5. Under Value, check **Item(s) from Match List**.
6. Under Match Lists, in the drop-down list, select the match list that contains the words and phrases that you want to filter, and then click **Add**.
7. On the Action tab, set the action options.
   See "Setting the action options for a content filtering rule" on page 132.
8. On the Action bar, click **Save**.
   When you are ready to process the rule, ensure that it is enabled on the Basics tab. In addition, ensure that rules processing is enabled on the Content Filtering > Rules tab.
   See "Enabling the content filtering process" on page 116.

Filtering content with word categories

Content filtering is typically used to monitor the mail system and block messages that contain specific types of content. Dictionary-based content filtering lets you filter the subject lines and bodies of messages by comparing their content against words in dictionary categories. Symantec Mail Security for Domino supplies categories and words, but you can also create your own.

For example, in most organizations, sending messages with explicit sexual or violent content is not considered an appropriate use of the mail system and violates corporate conduct guidelines. Dictionary categories such as Violence and Sex/Acts are designed to flag these types of messages by matching words in the message against words in the dictionary.

In addition, an organization might want to prevent the spread of confidential legal information outside of the organization. You can create custom word categories that include confidential terms and monitor messages for words in those categories. This helps ensure confidentiality and reduces possible legal liability.

How dictionary-based content filtering works

To evaluate content against your own custom words and categories or against the vendor (Symantec-supplied) words and categories, you build a content filtering rule using the Content Score attribute. In the rule, you assign one or more scores (thresholds) to one or more categories that you select. Symantec Mail Security for Domino then matches text in document writes and the subject lines and message bodies of email messages against words that belong to the set of selected categories. These words have predefined scores. The more strongly representative the word or phrase is of a particular category, the higher the score.

Symantec Mail Security for Domino assigns each document a score based on the total number of target words found. When a score exceeds your specified threshold for a particular expression in a rule, the content filtering engine considers that expression violated. The entire rule might be violated, depending on whether it contains OR expressions or AND expressions. When it contains OR expressions, a violation of any one expression violates the entire rule. When it contains AND expressions, all expressions in the rule must be violated before Symantec Mail Security for Domino flags the document as violating the entire rule. When an entire rule is violated, Symantec Mail Security for Domino takes action based on the action settings for the content filtering rule.

Content dictionaries and categories

Symantec Mail Security for Domino includes a dictionary, or repository, of commonly filtered words and phrases. These words and phrases are organized into categories against which you can run content filtering rules. (The contents of the vendor-supplied word categories are proprietary and cannot be viewed or modified.) You can also create your own custom word categories and words against which to filter. When you add a word or phrase to a custom word category that already exists in a vendor-supplied category, your custom entry supersedes the vendor-supplied entry. Custom words and categories are stored in sav.nsf, apart from the vendor-supplied database.

Whether you use the vendor-supplied categories of words or your own words and categories, you can select which categories of words to turn on or off for scoring in a content filtering rule. When Symantec Mail Security for Domino finds a word in a category that is turned off, it ignores it for the purposes of scoring.

Note: You can only create custom word categories in single-byte, ASCII characters. You can add words to that category in single-byte or multi-byte characters, but the words must be in the default language of the computer. Custom word category names are case-sensitive. The words or phrases that you add to a category are not case-sensitive.

Scoring messages

To score messages, Symantec Mail Security for Domino matches the individual words in a document against entries in the word categories. When a match is found, points are added to the message score. In addition, Symantec Mail Security for Domino examines successive words for use of contextual words, and adjusts the score accordingly. The sum total of points for the matches and surrounding words is the score for the document.

When the content filtering rule is enabled for the scan job in effect, Symantec Mail Security for Domino compares the message score against the threshold setting that you specify in the rule. When the message score is equal to or exceeds the threshold setting, the expression in the rule is violated.

Matching words and evaluating context

After the content filtering engine breaks the text block into words, it compares the extracted words in successive order to words in the word categories. Whenever a match with a word category entry occurs, a new process begins. The content filtering engine builds a word chain, which starts with the word that matches the word category entry.

The purpose of building a word chain is to further evaluate the meaning of a matched word by examining its context. For example, if the word cancer succeeds breast in a word chain, it is likely that the message is about a medical condition and is appropriate. By creating and evaluating word chain structures, the content filtering engine is able to catch these differences in meaning and adjust scoring accordingly.

Each word that follows the matched word is added to a chain until the following occurs:

- Two successive nondictionary words are found. At that point, the comparison process continues with the next word in the text block.
- The end of the block is reached. At that point, the processing of the next text block begins.

Calculating base and bonus scores

After Symantec Mail Security for Domino processes the document text, it calculates the total score for the message. This total score is cumulative across all enabled word categories. Symantec Mail Security for Domino does not produce scores for each word category separately.

Symantec Mail Security for Domino uses the following categories of scores when assigning values:

- Base score: The primary value that is assigned to a word or phrase

  Base scores can be positive or negative integers. The severity of a word's base score is relative to the scores of the other words in the category.
- Bonus score: A secondary value that is assigned to a word or phrase

  A bonus score can be positive or negative integers. Bonus scoring is used for word context and for adjustments to the total score. Only vendor-supplied words and phrases use bonus scores.

When you add a custom word or phrase to a custom word category, Symantec Mail Security for Domino requires that you assign a base score to the entry. It does not require a bonus score for custom entries.

Assigning the threshold values for scoring

Symantec Mail Security for Domino does not provide a default threshold value. You must choose a value for the content score rule, given the category or categories that you have configured for that rule.

For example, you might choose a value of 50 for the threshold value and choose the Comparison, > (greater than). This means that Symantec Mail Security for Domino must evaluate an email message as having a score of 51 or greater to trigger a rule violation. If you choose a threshold value of 20, for example, and a < (less than) Comparison, then a message score of 19 or less is necessary to trigger a violation.

The meaningfulness of the threshold value can vary widely. The content filtering engine correlates the total score with the total number of word matches in a document. Therefore, factors such as the number of word categories that you select for filtering and the file size affect the significance of the threshold value. The more word categories that you select and the larger the file size, the easier it is for a score to reach the threshold and trigger a content filtering rule violation.

When you create one or more rules that use the same group of categories more than once, Symantec Mail Security for Domino evaluates that group of categories against the email message only once. This optimizes performance.

When you create a rule with a combination of categories, for example, If Content Score > [50] using categories [sex;drugs;alcoholism] OR Content Score > [90] using categories [sex], then Symantec Mail Security for Domino evaluates the sex category twice.

Whenever rules contain duplicate combinations of categories across multiple rules or in the same rule, Symantec Mail Security for Domino filters content only once for any email message or document. Given all of the variables that can potentially affect document content scoring, you should test the content filtering rule before you put it into operation.

Use the following guidelines to test your content filtering rules:

- Use different threshold values, and observe the number of violations that are triggered.
- Use messages that contain known content violations that use different threshold settings, and observe whether the specific messages trigger rule violations.

Assigning scores to custom word categories

Part of the process of building custom word categories involves assigning scores to words. When you use custom word categories, you must do the following:

- Assign scores that accurately reflect the extent to which the word is representative of the category.
  A negative score can be used to offset the value of a prohibited word that is used in an appropriate context. For example, a negative score for the word cancer can offset the positive score of the word breast.
- Ensure that the threshold value for the content rule is set appropriately.

Use the following guidelines in choosing scores for custom words:

- Consider assigning a score of 25 to 50 when you are certain that the results will be found in the expected category, in which 50 represents absolute certainty. Assign a score of 0 to 25 based on the likelihood that a word will appear in the correct context.

- Test the words and categories against different threshold values in the content filtering rule, and adjust the word score or threshold values accordingly.

  If the default value of 50 is never attained and you are aware of several content filtering rule violations in a message that was passed over, consider lowering the threshold until the message is triggered, adding or rescoring the custom words, or removing existing words. Then, investigate which words trigger the content rule and their scores. Use this investigative work to fine-tune the content filtering rule settings so that the rule is reliably triggered.

Building a custom word category

Symantec Mail Security for Domino lets you build custom word categories to supplement the vendor (Symantec-supplied) word categories. Any custom words and categories that you create are added to a database that is separate from the vendor-supplied one. You can add any number of custom word categories and words.

You build custom word categories by adding new words, their scores, and the categories to which the words belong. You can assign words to a new, custom category or to an existing, vendor-supplied category. New words that are assigned to a vendor-supplied category are considered part of the custom word category and are stored separately from the vendor dictionary. In cases in which the same word is found in both dictionaries, the custom dictionary always takes precedence.

Symantec Mail Security for Domino uses the threshold value of the rule that contains the custom word category, and it ignores the threshold value that is supplied in the rule that contains the vendor category.

You view, add, edit, and delete custom words and categories, and you can add words to vendor-supplied categories.

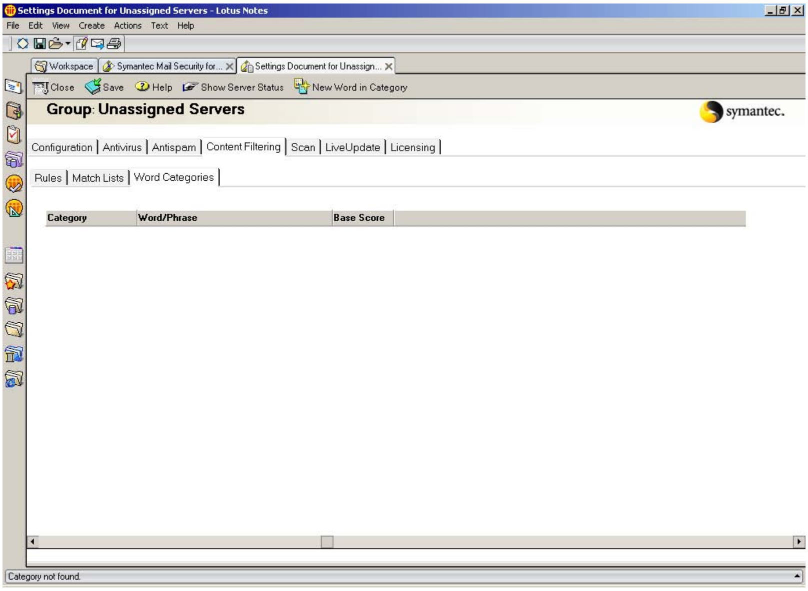
You must type a custom word category in ASCII characters. Category names cannot contain multi-byte characters. Category names are case-sensitive.

You can type custom words in English or in single-byte or multi-byte international characters, but the words must be in the default language of the computer. Custom words are not case-sensitive.

Omit commas when adding words or categories, or unpredictable results might occur.

To add a word or phrase to a word category

1 In the Group document, on the Content Filtering tab, click **Word Categories**.



Vendor-supplied word categories do not appear in this view. If you have not added any words or categories, the view is empty.

2 On the Action bar, click **New Word in Category**.

3 In the Content Filtering Word document, in the Category box, do one of the following:

- In the drop-down list, select a vendor-supplied category.
- Type a custom word category.

4 In the Word field, type a custom word or phrase for the category.

5 In the Base Score field, type a base score.
See "Calculating base and bonus scores" on page 139.

6 Under Servers, select one of the following:

- All servers in this group: Applies the word to all servers in the server group
  This option is enabled by default.
- The following servers: Applies the word to specific servers
  Select the servers from the drop-down list. Separate multiple entries with commas.

7 On the Action bar, click **Save**.

To edit a custom word, phrase, or word category name

1 In the Group document, on the Content Filtering tab, click **Word Categories**.

2 Under Word/Phrase, double-click the word or phrase that you want to edit.

3 In the Content Filtering Word document, make your revisions.

4 On the Action bar, click **Save**.

To delete a custom word or phrase

1 In the Group document, on the Content Filtering tab, click **Word Categories**.

2 Under Word/Phrase, double-click the word or phrase that you want to delete.

3 In the Content Filtering Word document, on the Action bar, click **Delete**.

4 In the confirmation dialog box, click **Yes**.

5 On the Action bar, click **Save**.
Symantec Mail Security for Domino automatically deletes the custom word category when all of the words or phrases within the category are deleted. Vendor-supplied word categories cannot be deleted.

Creating a content filtering rule that uses word categories

You create a content filtering rule that works with scored content by using the Content Score attribute to define the rule.

Before you define a content score rule, ensure that you understand dictionary-based content filtering and how Symantec Mail Security for Domino evaluates messages against the threshold values and categories that you specify in a content score rule.

See "Filtering content with word categories" on page 136.

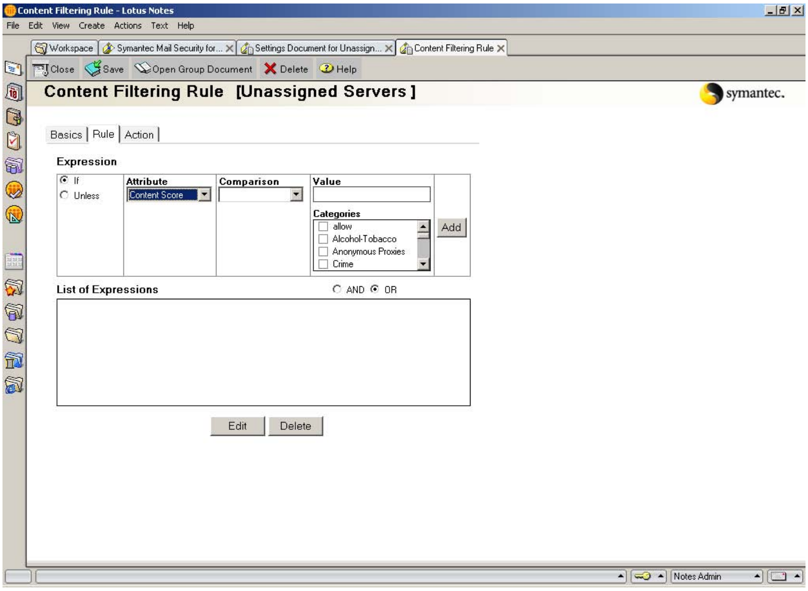
To create a content filtering rule that uses word categories

1 In the Group document, on the Content Filtering tab, click the **Rules** tab.

2 On the Action bar, click **New Rule**.

3 In the Content Filtering Rule document, on the Basics tab, set the basic options.
See "Setting the basic options for a content filtering rule" on page 119.

4 On the Rule tab, in the Attribute drop-down list, click **Content Score**.



5 In the Comparison drop-down list, select **>** (greater than) or **<** (less than).
If you select >, messages that score higher than your threshold value are considered content rule violations. If you select <, messages that score lower than your threshold value are considered rule violations.

6 In the Value box, type a threshold value.

Values can be positive or negative integers.

7 Under Categories, select one or more word categories that contain the repository of words against which the Content Score rule compares and matches, and then click **Add**.

The list provides both vendor-supplied and custom word categories.

8 On the Action tab, set the action options.

See "Setting the action options for a content filtering rule" on page 132.

9 On the Action bar, click **Save**.

When you are ready to process the rule, ensure that rules processing is enabled on the Rules tab.

See "Enabling the content filtering process" on page 116.

Filtering spam

This chapter includes the following topics:

About spam filtering

Symantec Mail Security for Domino protects your servers from unwanted email messages, such as spam. Spam messages are unsolicited bulk email messages that typically contain advertising. Symantec Mail Security for Domino scans the contents of incoming email messages to determine the likelihood that they are spam.

Symantec Mail Security for Domino provides the following types of antispam scanning functionality:

Standard antispam	Standard antispam uses a pattern-matching, heuristics engine to compare the contents of incoming email messages to a list of spam characteristics. You can select the antispam engine sensitivity level. You can also prepend the email subject line to tag the message as spam and add the accuracy percentage to the email message. See "Configuring standard antispam settings" on page 152.

Premium antispam service	The Symantec Premium AntiSpam service provides continual, real-time updates to the Symantec Premium AntiSpam filters. This ensures that your Domino server has the most current spam detection filters that are available. See "Identifying spam using the premium antispam service" on page 157. Additional configuration may be required to ensure that your environment supports the premium antispam service. See "Before you install and enable the premium antispam service" on page 153. You can configure Symantec Premium AntiSpam to automatically route spam messages to a spam folder in the recipient's mailbox. See "Disposing of spam messages using premium antispam" on page 163. See "Automatically routing messages to a spam folder" on page 231.

The white list feature lets you specify domains that are permitted to bypass antispam scanning. This can reduce the incidents of false positives. The standard antispam engine and the premium antispam service share the white list.

See "Managing a white list" on page 149.

You can configure the product to log spam events as follows:

Log events to the Symantec Mail Security for Domino Log.	See "Enabling spam event logging" on page 150.
Log events to the operating system event log.	See "Configuring logging options" on page 88.
Log events to SESA.	See "Integrating Symantec Mail Security for Domino with SESA" on page 237.

Managing a white list

The white list helps you prevent legitimate email messages from being incorrectly identified as spam (false positives). You can add domains to the white list to ensure that standard business email messages are delivered without unnecessary delay.

Email messages from domains that are contained in the white list bypass antispam scanning. However, they are scanned for viruses and content filtering rule violations according to the scanning policies that you configure.

See “Establishing antivirus scanning policies” on page 104.

See “Working with content filtering rules” on page 115.

You can use absolute Internet domain names or base domain names. Mailer1.domain.com and mailer2.domain.com are examples of absolute domain names. When you add these absolute domain names to the white list, email messages from these addresses bypass antispam scanning. However, an email message from mailer3.domain.com would be scanned for spam. Domain.com is an example of a base domain name. When you add this base domain to the white list, any email message from any domain.com address bypasses antispam scanning.

To manage a white list, you should consider implementing a process to collect false positives that are reported by users. Each case can be analyzed and domains can be added to a white list to prevent false positives from these sources in the future.

To add an address to a white list

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam tab, on the White List tab, under Antispam white list exclusion, check **Bypass antispam using white list**.
3. To add a domain to the white list, click **Add/Edit antispam white list domain(s)**.
4. In the Add/Edit antispam white list domain(s) dialog box, type the Internet domain addresses that you want to exclude from antispam scanning.

   Separate entries with a comma or semicolon or by creating a new line.

   The premium antispam service does not support high ASCII or double- byte characters.
5. When you are finished, click **OK**.

   The domain addresses appear in the Exclude the following white list domains box.
6. On the Action bar, click **Save**.

To delete an address from the white list

1 In the Settings view, double-click a server group.

2 In the Group document, on the Antispam tab, on the White List tab, in the Exclude the following white list domains box, click the domains that you want to delete from the white list.
A check mark appears to the left of the domains that you select.

3 Click **Remove selected antispam white list domain(s)**.

4 On the Action bar, click **Save**.

Enabling spam event logging

Symantec Mail Security for Domino lets you log spam events that are detected by the standard antispam engine and premium antispam service. You can log events to any of the following locations:

Log events to the Symantec Mail Security for Domino Log.	See "Enabling spam event logging" on page 150.
Log events to the operating system event log.	See "Configuring logging options" on page 88.
Log events to SESA.	See "Integrating Symantec Mail Security for Domino with SESA" on page 237.

See "Configuring logging options" on page 88.

Note: Spam or suspected spam messages that are deleted by the premium antispam service are not logged to any of the logging locations or included in spam email statistics.
See "Understanding the Log views" on page 197.

To enable spam event logging

1 In the Settings view, double-click a server group.

2 In the Group document, on the Antispam tab, on the Basics tab, check **Log spam events**.

3 On the Action bar, click **Save**.

Identifying spam using the standard antispam feature

The standard antispam feature uses a pattern-matching engine to compare the contents of incoming email messages to a list of spam characteristics. A message that contains many spam characteristics is more likely to be spam than a message that contains few spam characteristics. Based on this analysis, Symantec Mail Security for Domino estimates the likelihood that the message is spam.

Symantec Mail Security for Domino lets you configure the threshold for marking an email message as spam. When you set the antispam detection level to Low, messages must contain many spam characteristics before they are flagged as spam. When you set the level to High, messages that contain only a few spam characteristics are flagged.

The standard antispam engine only scans email messages that are received from Internet email addresses for spam characteristics. Internal email messages bypass antispam scanning, which conserves system resources.

The white list feature lets you specify domains that are permitted to bypass antispam scanning. This reduces the incidents of false positives.

See "Managing a white list" on page 149.

You can configure the product to log spam events as follows:

Log events to the Symantec Mail Security for Domino Log.	See "Enabling spam event logging" on page 150.
Log events to the operating system event log.	See "Configuring logging options" on page 88.
Log events to SESA.	See "Integrating Symantec Mail Security for Domino with SESA" on page 237.

Configuring standard antispam settings

Symantec Mail Security for Domino performs an analysis of the entire incoming email message for key characteristics of spam. It weighs its findings against key characteristics of legitimate email messages and assigns an accuracy rating (for example, 98%) about the certainty that the message is spam. The rating, in conjunction with the engine sensitivity level, determines whether a message is considered spam.

You can adjust the sensitivity of the antispam engine to maximize detections and minimize false positives. The sensitivity threshold can be set from 1 (low) to 5 (high), where 1 minimizes false positives (and detections), and 5 maximizes detections (and false positives). The default sensitivity level for the antispam engine is 1 (Low). When you increase the sensitivity level, more false positives are likely to occur.

You can prepend the subject line of the email message to notify the recipient that the email message is identified as spam. You can also add a field to the email message that provides the spam detection accuracy percentage. After an email message is scanned, it is routed to the intended recipient.

Note: To use standard antispam, you must have a valid product license.

See "Activating your Symantec Mail Security for Domino licenses" on page 61.

To configure standard antispam settings

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam tab, on the Basics tab, **check Enable spam detection**.
3. On the Standard tab, under Engine sensitivity level, in the drop-down list, select the sensitivity level of the antispam engine.
   The default level is: 1 (Low).
4. To add a new field in the header, under Spam mail header, check **Add new header**.
5. In the Header text field, type the header field name.
   The default header field name is X_Bulk.
6. To prepend the subject line text, under Spam mail subject, check **Prepend to the subject**, and then type your customized text message.
   The default text is: Spam.
   When no text is typed in the box, the subject line is not modified.
7. On the Action bar, click **Save**.

Before you install and enable the premium antispam service

When a Lotus Domino server receives an incoming email message, Domino SMTP Inbound converts the email message into a note or a document. During this enumeration process, Domino removes the raw SMTP information from the email message. Symantec Premium AntiSpam requires the raw SMTP information to identify potential spam messages. As a result, the premium antispam service must scan email messages before they reach Domino SMTP Inbound.

The solution is to use the Microsoft SMTP service (which is a component of Microsoft Internet Information Services [IIS]) to intercept email messages before they reach Domino SMTP Inbound and route them to the premium antispam service for scanning. The premium antispam service scans the raw SMTP information and determines if the email message is spam, suspected spam, or not spam. Depending on your configuration, email messages are deleted or forwarded by Microsoft SMTP to Domino SMTP Inbound for further processing.

See “Disposing of spam messages using premium antispam” on page 163.

You must install the Microsoft SMTP service and IIS Administration before you install Symantec Mail Security for Domino. When you install Symantec Mail Security for Domino, the program installer detects the IIS services that are enabled on your computer. It prompts you to disable unnecessary services. Disabling unnecessary IIS services hardens Microsoft IIS and protects your Domino server from being compromised.

You must install Symantec Mail Security for Domino on each computer on which you intend to use the premium antispam service and enable the premium antispam service. You can enable the premium antispam service only once per computer. If you have multiple Lotus Domino partitions on the same computer, you must choose the partition on which you want to enable the premium antispam service.

See “Enabling and disabling the premium antispam service” on page 159.

See “Specifying internal mail hosts” on page 162.

When you enable the premium antispam service, Symantec Mail Security for Domino configures the Microsoft SMTP service to function like SMTP Inbound. Symantec Mail Security for Domino also configures the Microsoft SMTP service to receive email on behalf of the Domino server and to forward that email to Domino SMTP Inbound after the antispam scanning.

If the premium antispam service is disabled or if the premium antispam service license expires, Symantec Mail Security for Domino disables the Microsoft SMTP service and changes the configuration parameters of Domino SMTP Inbound to receive inbound messages directly. The Microsoft SMTP settings are copied to Domino SMTP Inbound. This restoration process ensures that your Domino environment is not disrupted.

Constraints in using the premium antispam service

Table 8-1 describes the constraints in using the premium antispam service.

Table 8-1 Premium antispam service constraints

Constraint	Description
SMTP relaying is disabled.	When you use a Domino server for relaying, you configure it to permit the relaying of email messages from specific hosts based on their IP addresses. However, when you enable the premium antispam service, external hosts connect to the Microsoft SMTP service. Domino SMTP Inbound is unable to differentiate between hosts that are permitted to relay and hosts that are not. To protect your Domino server from an insecure, open relay, Symantec Mail Security for Domino disables all SMTP relaying.
All Configuration document changes must be made in the Server Configuration document.	When you enable the premium antispam service, Symantec Mail Security for Domino creates a Server Configuration document, if one does not exist. Symantec Mail Security for Domino copies the settings that it detects in global and group Configuration documents to the Server Configuration document. Thereafter, changes to global and group Configuration documents will not apply to the server. All changes must be made in the Server Configuration document.
Domino 6x Site Documents are not supported.	The premium antispam service does not support the use of Site Documents. You must disable the Site Documents feature to use the premium antispam service.
High ASCII and double-byte characters are not supported.	The premium antispam service does not support high ASCII or double-byte characters for the following: ■ White list domains ■ Email subject line prepend text ■ Directories and folders

Table 8-1 Premium antispam service constraints

Constraint	Description
Microsoft SMTP service cannot be used for any purpose other than the premium antispam service.	When you install and enable the premium antispam service, Symantec Mail Security for Domino takes control of the Microsoft SMTP service and removes any existing configurations. Symantec Mail Security for Domino does not permit using the Microsoft SMTP service for any purpose other than the premium antispam service.

Lotus Domino setup considerations

Table 8-2 describes the tasks that you might have to perform in Lotus Domino if you use certain features with the premium antispam service.

Table 8-2 Domino feature tasks

Domino feature	Task
Domino R5 console commands	Symantec Mail Security for Domino runs as a server task on your Domino server using the same identity and authority of the server. By default, Domino R5 does not permit the server to use the remote console facility to send remote console commands to itself. However, Symantec Mail Security for Domino relies on remote console commands to enable and run the premium antispam service. To use the premium antispam service on Domino R5, you must list the name of the Domino server or the group to which the server belongs in the Administrators field in the Server document. Removing the Domino server from the Administrators field when the premium antispam service is enabled results in a server failure. For more information, see your Lotus Domino documentation.

Table 8-2 Domino feature tasks

Domino feature	Task
IP address connection allow/ deny lists	When you enable the premium antispam service, Symantec Mail Security for Domino automatically copies the settings in the Domino SMTP Inbound allow/deny lists to the Microsoft SMTP service. If you need to modify these settings, you can do one of the following: ■ Make the modifications in Microsoft SMTP. If you disable the premium antispam service, Symantec Mail Security for Domino deletes any existing settings in the Domino allow/deny lists and replaces them with the settings in the Microsoft SMTP allow/deny lists. ■ Disable the premium antispam service, make the changes in Domino Administrator, and then re-enable the premium antispam service. When the premium antispam service is re-enabled, Symantec Mail Security for Domino deletes any existing settings in the Microsoft SMTP allow/deny list and replaces them with the settings from the Domino allow/deny lists.

Expected behaviors in using the premium antispam service

Table 8-3 describes the behavior that you can expect when you enable, disable, and use the premium antispam service.

Table 8-3 Expected behaviors

Behavior	Description
Enabling and disabling the premium antispam service requires a few minutes to process.	When you enable the premium antispam service, Symantec Premium AntiSpam must connect to the Symantec Brightmail Logistics and Operations Center (BLOC) and download the current antispam filters. Depending on your connection speed and available bandwidth, this process could take a few minutes. Disabling the premium antispam service requires Symantec Mail Security for Domino to reconfigure internal settings, which takes a few minutes to process.
Console error messages appear when enabling and disabling the premium antispam service.	Disregard error messages that occur while enabling or disabling the premium antispam service. This behavior is normal and should be expected.

Table 8-3 Expected behaviors

Behavior	Description
A new port appears on the Ports tab and in the Notes.ini file.	When you enable the premium antispam service, if Symantec Mail Security for Domino does not detect a port that is bound to the correct address, it creates one called SMSDOMPAS on the Ports tab of the Server document and in the Notes.ini file. Do not use SMSDOMPAS for any other purpose. If the premium antispam service is disabled, SMSDOMPAS still appears on the Ports tab, but it is disabled. It is removed from the Notes.ini file.

Identifying spam using the premium antispam service

Symantec Premium AntiSpam is a subscription service that provides enhanced spam detection. Continuous updates to the premium antispam filters ensure that your Domino server has the most current spam detection filters that are available. Updates to the premium antispam service are handled through the Symantec Premium AntiSpam service and not through LiveUpdate. Updates to the premium antispam filters are not stored in a Domino database, so they cannot be replicated.

Symantec Premium AntiSpam uses the following to identify and handle spam:

Filters

Symantec Probe Network is a global network of decoy email addresses that attracts and collects the latest spam. When spam is received, the Symantec Brightmail Logistics and Operations Center (BLOC) issues filters that isolate similar spam messages.

Symantec builds its known-spammer list based on the URLs that appear in spam messages that are collected by the Symantec Probe Network.

Symantec downloads a list of MIME filters developed by BLOC and treats any message as spam if any MIME attachment in the message matches a Symantec MIME filter.

Reputation service

Symantec monitors email sources to determine how much of the email messages that are sent from those sources is legitimate. Email from those sources can then be blocked or allowed based on the reputation value of the source as determined by Symantec.

See “Disabling the reputation service lists” on page 161.

Suspected spam threshold	Symantec calculates a spam score from 1 to 100 for each message. If a message scores from 90 to 100, it is defined as spam. For more aggressive filtering, you can define a spam threshold below 90 and above 24 to identify suspected spam. See "Adjusting suspected spam scoring in premium antispam" on page 160.
Spam disposition	Symantec Mail Security for Domino lets you choose how to dispose of spam and suspected spam email messages. See "Disposing of spam messages using premium antispam" on page 163.

The white list feature lets you specify domains that are permitted to bypass antispam scanning. This reduces the incidents of false positives.

See "Managing a white list" on page 149.

You can configure the product to log spam events as follows:

Log events to the Symantec Mail Security for Domino Log.	See "Enabling spam event logging" on page 150.
Log events to the operating system event log.	See "Configuring logging options" on page 88.
Log events to SESA.	See "Integrating Symantec Mail Security for Domino with SESA" on page 237.

To use the premium antispam service, you must have a product license and a Symantec Premium AntiSpam license.

See "Activating your Symantec Mail Security for Domino licenses" on page 61.

If you use the premium antispam service and your license expires or the premium antispam service is disabled, the standard antispam feature is automatically activated, provided that the following conditions are met:

- You have enabled spam detection.
  See "Enabling and disabling the premium antispam service" on page 159.
- You have a current product license.
  See "Activating your Symantec Mail Security for Domino licenses" on page 61.

Enabling and disabling the premium antispam service

Before you enable the premium antispam service, do the following:

- Ensure that your environment meets the requirements for installing and enabling the premium antispam service.
  See "Before you install and enable the premium antispam service" on page 153.
- Activate the product and Symantec Premium AntiSpam licenses.
  See "Activating your Symantec Mail Security for Domino licenses" on page 61.

You can enable the premium antispam service on one Domino partition per computer. If you intend to use the premium antispam service on a partitioned server, you must choose the partition on which you want to enable the premium antispam service. You must disable the premium antispam service that is running on a partition before you enable it on a different partition.

You can replicate the Settings database to multiple Domino servers that are running Symantec Mail Security for Domino. The subset of the servers that are licensed to run the premium antispam service appears on the AntiSpam > Premium AntiSpam > Control tab.

For each server in the server list, Symantec Mail Security for Domino indicates whether the premium antispam service is enabled or disabled. When you enable or disable the premium antispam service on a server, the status of that server changes in the server list. This change does not appear in other replicas of the Settings database until after the next replication occurs. It may take a few minutes to enable or disable the premium antispam service.

Note: When you enable or disable the premium antispam service using a remote replica of that server's Settings database, the server on which you are enabling or disabling the service and the server on which the replica resides must be able to communicate over the network throughout the process. Otherwise you might see error messages or experience delays.

If an error occurs when you enable or disable the premium antispam service, the server list provides information about why the failure occurred. If the premium antispam service is automatically disabled due to an error or license expiration, the server list in the server's local replica of the Settings database provides information about why the service was disabled. In either instance, this information appears in the other replicas after the replication process occurs.

Warning: Stopping the Domino server while enabling or disabling the premium antispam service results in server failure.

To enable the premium antispam service

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam tab, on the Basics tab, **check Enable spam detection**.
3. On the Antispam > Premium AntiSpam > Control tab, double-click the server on which you want to enable the premium antispam service.
4. In the confirmation dialog box, click **OK**.
5. On the Action bar, click **Save.**

To disable the premium antispam service

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam > Premium AntiSpam **>** Control tab, double-click the server on which you want to disable the premium antispam service.
3. In the confirmation dialog box, click **OK**.

Adjusting suspected spam scoring in premium antispam

Symantec Premium AntiSpam calculates a spam score from 1 to 100 for each email message that it scans to evaluate whether the message is spam. This evaluation is based on pattern matching techniques and heuristic analysis. If an email message scores in the range of 90 to 100, the premium antispam service defines the email message as spam. The score range cannot be modified. However, you can define the range for which email messages are considered suspected spam and not spam.

You can also specify different actions for messages that are identified as suspected spam and spam.

See "Disposing of spam messages using premium antispam" on page 163.

To adjust suspected spam scoring in premium antispam

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam > Premium AntiSpam **>** Spam Scoring tab, under Flag messages as suspected spam, click **Yes** to enable detection of suspected spam.

3 In the Suspected spam message score list, select the minimum value for the range in which the premium antispam service defines suspected spam email.
Messages that score within this range are considered suspected spam.
The minimum value is 72.

4 On the Action bar, click **Save**.

Disabling the reputation service lists

Symantec monitors hundreds of thousands of email sources worldwide to determine how much of the email that is sent from these addresses is legitimate and how much is spam. The reputation service lists are continuously compiled and updated into the premium antispam service.

The reputation service includes the following lists:

Open Proxy List	IP addresses that are open proxies used by spammers
Safe List	IP addresses from which virtually no outgoing email is spam
Suspect List	IP addresses from which virtually all of the outgoing email is spam

By default, Symantec Premium AntiSpam uses the reputation service. No configuration is required for these lists. You can choose to disable the Open Proxy List or the Safe List. The Suspect List is always enabled.

To disable the reputation service lists

1 In the Settings view, double-click a server group.

2 In the Group document, on the Antispam > Premium AntiSpam > Reputation Service tab, under Select the reputation service list(s) to use, uncheck the lists that you do not want to use.
The Suspect List is always enabled.

3 On the Action bar, click **Save**.

Specifying internal mail hosts

To provide accurate source-based filtering, the premium antispam service must know which IP addresses are internal to your organization and which are external. You must specify the IP address of any email server in your organization that might intercept an email message before it reaches the server on which the premium antispam service is running.

If you enable the premium antispam service anywhere besides the gateway, you must provide information about your internal mail network. Symantec Premium AntiSpam uses this information to extract the logical connection address of the mail message. The logical connection address is the IP address of the SMTP server that sent the email message to your organization. In non-gateway environments, Symantec Premium AntiSpam uses this logical connection to match these addresses with the IP connections that are specified in the white list or the safe list that is provided by the reputation service.

To specify the server location

1. In the Settings view, double-click a server group.
2. If all of the servers in the server group on which you have enabled the premium antispam service are at the messaging gateway, in the Group document, on the Antispam > Premium AntiSpam > Internal Mail Hosts tab, under Server location, check **All Premium AntiSpam enabled servers in this group are at the message gateway**.
   This option is checked by default.
3. On the Action bar, click **Save**.

To add an internal mail host

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam > Premium AntiSpam > Internal Mail Hosts tab, click **Add/Edit internal mail host(s).**
3. Type the IP address, IP address range, or host name.
4. Click **OK**.
5. On the Action bar, click **Save**.

To delete an internal mail host

1 In the Settings view, double-click a server group.

2 In the Group document, on the Antispam > Premium AntiSpam > Internal Mail Hosts tab, in the Internal mail hosts list, select the internal mail host that you want to delete.
A check mark appears to the left of the internal mail hosts that you select.

3 Click **Remove selected internal mail host(s)**.

4 On the Action bar, click **Save**.

Disposing of spam messages using premium antispam

You can specify different actions for messages that are identified as spam and suspected spam. For example, assume that you have configured your suspected spam scoring range to encompass scores from 80 to 89. If an incoming message receives a spam score of 89, Symantec Premium AntiSpam considers this message to be suspected spam. It then applies the action that you have in place for suspected spam messages, such as Modify Message.

See “Adjusting suspected spam scoring in premium antispam” on page 160.

You can configure the premium antispam service to automatically route messages to a spam folder in the recipient’s mailbox. To use this feature, you must install the foldering agent, which is available on the Symantec Mail Security for Domino installation CD.

See “Automatically routing messages to a spam folder” on page 231.

To dispose of spam email messages

1. In the Settings view, double-click a server group.
2. In the Group document, on the Antispam > Premium AntiSpam > Actions tab, under When Spam is detected, select one of the following:

Delete the document

Deletes the email message.

Spam messages that are deleted by the premium antispam service are not logged to any of the logging locations or included in spam statistics.

Deliver the document

Delivers the email message to the inbox folder of the recipient.

Deliver the document to recipient’s spam folder

Delivers the email message to the spam folder of the recipient.

This option requires that you install the foldering agent.

See “Automatically routing messages to a spam folder” on page 231.

Modify Message

Lets you modify the X-header and subject line of the email message.

Do any of the following:

- Click **Add X-header** and type the X-header that you want to use.
  The X-header must use the following format: X-[header]:[value]. X-headers that begin with X-SYM or X-BMI are reserved for Symantec Mail Security for Domino and cannot be used. The X-header does not support semicolons or spaces.
- Click **Prepend the subject** and type your customized text message.
  The default text is Spam. The premium antispam service does not support the use of high ASCII or double-byte characters.

3 Under When Suspected Spam is detected, select one of the following:

Delete the document

Deletes the email message.

Spam messages that are deleted by the premium antispam service are not logged to any of the logging locations or included in spam statistics.

Deliver the document

Delivers the email message to the inbox folder of the recipient.

Deliver the document to recipient's spam folder

Delivers the email message to the spam folder of the recipient.

This option requires that you install the foldering agent.

See "Automatically routing messages to a spam folder" on page 231.

Modify Message

Lets you modify the X-header and subject line of the email message.

Do any of the following:

- Click **Add X-header** and type the X-header that you want to use.
  The X-header must use the following format: X-[header]:[value]. X-headers that begin with X-SYM or X-BMI are reserved for Symantec Mail Security for Domino and cannot be used. The X-header does not support semicolons or spaces.
- Click **Prepend the subject** and type your customized text message.
  The default text is Spam. The premium antispam service does not support the use of high ASCII or double-byte characters.

Chapter 9

Scanning for viruses, spam, and content filtering rule violations

This chapter includes the following topics:

About scanning

Symantec Mail Security for Domino uses several antivirus technologies to scan documents for viruses. It looks for known viruses by comparing segments of your documents to the sample code inside of a virus definition file. The virus definition file contains nonmalicious bits of code, or virus definitions, for numerous known viruses. When Symantec Mail Security for Domino finds a match, the document is considered infected, and the document is disposed (repaired, deleted, quarantined, or logged and delivered) according to your configuration settings. When Symantec Mail Security for Domino receives an email message with an attachment from an Internet source, it decodes and decompresses the attachment and then scans it for viruses.

Symantec Mail Security for Domino also uses Symantec Bloodhound heuristics technology to scan for viruses for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors, such as self-replication, to target potentially infected documents.

The standard antispam feature uses a pattern-matching, heuristics engine to compare the content of incoming email messages to a list of spam characteristics. You can select the antispam engine sensitivity level. If you subscribe to the premium antispam service, the Symantec Premium AntiSpam service provides continual, real-time updates to the Symantec Premium AntiSpam filters to ensure that your Domino server has the most current spam detection filters that are available. Standard antispam and the premium antispam service use the white list feature to reduce the incidents of false positives.

Symantec Mail Security for Domino lets you filter undesirable message content by using dictionary-based content filtering and content filtering rules that you create.

Symantec Mail Security for Domino scans first for viruses, then for spam detection, and then for content filtering rules.

To perform any of the Symantec Mail Security for Domino scanning functions, you must have a valid product license installed.

See "About licensing" on page 61.

Symantec Mail Security for Domino can perform the following types of scans:

- Auto-protect: Detects viruses in real-time as email messages and documents are routed through the Lotus Domino server
  See "About auto-protect scanning" on page 168.
- Scan now: Lets you perform a scan on-demand
  See "About scan now scanning" on page 170.
- Scheduled scan: Lets you configure Symantec Mail Security for Domino to scan the Domino server on a regular schedule
  See "About scheduled scanning" on page 174.

About auto-protect scanning

Auto-protect provides continuous protection against viruses, spam, and content filtering rule violations. When you enable auto-protect scanning, Symantec Mail Security for Domino scans email messages as they pass through the Domino server and scans documents as they are written. Infected documents, spam messages, and content filtering rule violations are detected on a real-time basis.

If you turn off the auto-protect scanning feature, viruses, spam, and content filtering rule violations can only be detected by performing a scheduled scan or a scan now scan. The auto-protect feature (for email routing and document writes) is enabled by default to provide you with the most secure settings upon installation.

Warning: Turning off the auto-protect feature leaves your server vulnerable to attacks. You should keep this feature enabled.

Configuring auto-protect settings

With auto-protect continuous scanning, you can monitor email routing and document writes. You can also identify which server processes to ignore. You should not remove the default processes from the list of processes to ignore.

To configure auto-protect settings

1. In the Settings view, double-click a server group.
2. In the Group document, on the Configuration tab, on the Auto-Protect tab, under Enable Scanning for, select any of the following:
   - Email routing
     The premium antispam service continues to scan email messages when this option is disabled.
     See "Before you install and enable the premium antispam service" on page 153.
   - Document writes

   Both options are enabled by default.
3. To modify the default list of processes to ignore, under Ignore the following server processes, do any of the following:
   - Type the process that you want to add to the list.
   - Delete the process that you want to remove from the list.

   By default, Symantec Mail Security for Domino excludes compact, fixup, updall, and update. It automatically excludes Symantec Mail Security for Domino processes.
   Reset to defaults returns the server processes to the default settings.
4. On the Action bar, click **Save**.

About scan now scanning

In addition to auto-protect and scheduled scanning, you can perform a server scan on-demand. Scan now scans let you scan all of the databases in the default data directory or specific directories that you select. You specify which exclusions to apply, how to handle attachments, whether to scan native MIME message bodies, whether to scan for content filtering rule violations, whether to scan all documents or only those that were modified since a specified date, and how to respond when a virus is detected.

You can perform a scan now scan through the user interface or from the Domino console.

See "Initiating tasks from the Domino console" on page 56.

See "Configuring scan now settings" on page 171.

To scan for content filtering rule violations, you must first specify that the content filtering rule applies to Manual Scans (scan now) when you create or modify a rule.

See "Setting the basic options for a content filtering rule" on page 119.

Warning: Scanning for content filtering violations is not safe for most databases. Only apply content filtering rules to databases that need to be scanned for a specific type of content filtering rule violation.

For incremental scans, Symantec Mail Security for Domino uses the current date format that is set on the system, regardless of what is typed. For example, if you type 5/3/04 12 A.M., and the date format on your computer is set for MM/DD/YY HH:MM AM/PM, Symantec Mail Security for Domino reflects the date as 05/03/04 12:00 A.M.

You can also configure Symantec Mail Security for Domino to dispose of documents that contain violations. When Symantec Mail Security for Domino deletes an attachment, it adds explanatory text to the attachment icon. By default, it saves the deleted attachment as a backup document in the Quarantine. When scan now scanning is enabled, if Symantec Mail Security for Domino detects a virus inside a container file, it deletes the container file and everything in it. When a container file is comprised of both infected and uninfected files, the entire container file and all the files inside it might be deleted.

If you choose to quarantine infected documents, you must open those documents in the Quarantine to process the infected documents. You must have the appropriate Role assignments to view quarantined documents.

See "About releasing documents from the Quarantine" on page 219.

See "Assigning Quarantine roles" on page 216.

Configuring scan now settings

You can change settings as necessary to run scan now scans. After you configure a scan now scan, you can run it at any time by clicking Start the Scan on the Action bar of the Scan Now tab.

Configure scan now settings

To configure scan now scans, set the following options:

- Basics: Defines which directories and subdirectories are included in the scan
- What to Scan: Contains settings for which types of attachments to scan, whether to perform content filtering, whether to scan native MIME message bodies, and the dates and time to perform incremental scans
- Actions: Specifies how to dispose of infected documents that are found during the scan

To configure scan now basic settings

1. In the Settings view, double-click a server group.
2. In the Group document, on the Scan > Scan Now > Basics tab, under What to scan on the server <server name>, select one of the following:
   - All databases in the default data directory: Scans every database in the Domino\Data directory (default location) for each server in the server group
     This option is enabled by default.
   - The following databases and directories: Scans only the databases and directories that you specify
     Type the database and directories to scan. Separate multiple entries with semicolons (;).
3. To scan subdirectories, check **Include subdirectories**.
   Enabling this option scans the descending subdirectories of the default data directory or the directories that you specified.
   This option is enabled by default.
4. On the Action bar, click **Save**.

To configure scan now what to scan settings

1. In the Group document, on the Scan tab, on the Scan Now tab, click the **What to Scan** tab.
2. To exclude specific databases or directories from the scan, under Databases, check **Exclude specified databases and directories from scan**.

   You must first select these databases and directories on the Configuration > Inclusions/Exclusions tab.

   See "Specifying what to scan" on page 84.

   This option is enabled by default.
3. Under Attachments, select one of the following:
   - Scan all attachments regardless of extension: Scans all attachments

     This option provides the greatest protection against virus attacks and is enabled by default.
   - Scan attachments with specified file extensions: Scans only those attachments with file name extensions that are listed in the Specified file extensions option on the Configuration > Inclusions/Exclusions tab
4. To scan for content filtering rule violations, under Content Filtering, check **Scan for Content Filtering rule violations**.

   Scanning for content filtering violations is not safe for most databases. Only apply content filtering rules to databases that need to be scanned for a specific type of content filtering rule violation.
5. To scan native MIME message bodies, under Scan Native MIME message bodies, click **On.**
6. To limit the scan to documents that are modified after the date that you select, under Incremental Scan, check **Scan only documents modified since**.
7. Type the date and time for the incremental scan.

   Symantec Mail Security for Domino uses the current date format that is set on the system, regardless of what is typed.
8. On the Action bar, click **Save**.

To configure scan now actions settings

1 In the Group document, on the Scan > Scan Now > Actions tab, under When a virus is detected, select one of the following:

Log only	Logs the detection but leaves the virus untreated.
Delete the infected attachment	Strips the infected attachment, making it unrecoverable.
Quarantine the document	Holds the infected document in the Quarantine for administrator review.
Repair the infected attachment	Automatically eliminates the virus and repairs any damage. When Symantec Mail Security for Domino cannot repair the document, the selected If unable to repair option applies. This option is enabled by default.

2 Under If unable to repair, select one of the following:

- Log only
- Delete the infected attachment
- Quarantine the document
  This option is enabled by default.

3 On the Action bar, click **Save**.

To scan now

1 In the Settings view, double-click a server group.

2 In the Group document, on the Scan tab, on the Action bar, click **Start the Scan**.

3 On the Scan Status document, on the Action bar, click **Check Scan Status**.
See "Scan status errors" on page 54.

4 If you need to stop the scanning process before it finishes, on the Action bar, click **Stop the Scan**.

5 To return to the Scan Now tab, click **Close**.

About scheduled scanning

You can schedule scans to repeat at the same time on specified days or at a specified interval on specified days.

To configure a scheduled scan, you specify the days and times to run the scan, including whether to run it after a successful virus definitions update with LiveUpdate. (To receive updated virus definitions, you must have a valid content license and have enabled LiveUpdate.)

See "Activating your Symantec Mail Security for Domino licenses" on page 61.

See "Configuring LiveUpdate" on page 181.

You can also specify which databases and directories to scan, which exclusions to apply, how to handle attachments, whether to scan for content filtering rule violations and native MIME message bodies, whether to scan all documents or only those that were modified since the last scheduled scan, and how to respond when a virus is detected. You can enable or disable a scheduled scan and specify which servers to scan in a server group.

To scan for content filtering rule violations, you must first specify that the content filtering rule applies to Scheduled Scans when you create or modify a rule.

See "Setting the basic options for a content filtering rule" on page 119.

Warning: Scanning for content filtering violations is not safe for most databases. Only apply content filtering rules to databases that need to be scanned for a specific type of content filtering rule violation.

By default, the Unassigned Servers server group is configured to run scheduled scans daily between 04:00 A.M. and 06:00 A.M., but you can modify these settings. (This scan is turned off by default.)

You choose when you want the scan to begin and end. When you enter a time range, for example, 04:00-06:00 A.M., the scan starts at 04:00 A.M. and ends at 06:00 A.M., even if it is not finished scanning all of the databases that it is configured to scan. When a scan has remaining databases to examine at its stop time, it continues where it left off at the next scheduled time. When you enter a single time, for example, 9:00 A.M., the scan always continues until it is completed, regardless of the time required to do so.

For incremental scans, Symantec Mail Security for Domino uses the current date format that is set on the system, regardless of what is typed. For example, if you type 5/3/04 12 A.M., and the date format on your computer is set for MM/DD/YY HH:MM AM/PM, Symantec Mail Security for Domino reflects the date as 05/03/04 12:00 A.M.

Note: For domains with multiple servers, Symantec Mail Security for Domino lets you schedule the same scan to run on one or more servers. You can schedule the scan itself from any server in the domain. For server-specific changes to scheduled scans, the Settings database (sav.nsf) must be replicated to the appropriate servers.
See "Managing multiple servers" on page 74.

You can also configure Symantec Mail Security for Domino to dispose of documents that contain violations. When Symantec Mail Security for Domino deletes an attachment, it adds explanatory text to the attachment icon. By default, it saves the deleted attachment as a backup document in the Quarantine. When scheduled scanning is enabled, if Symantec Mail Security for Domino detects a virus inside a container file, it deletes the container file and everything in it. When a container file is comprised of both infected and uninfected files, the entire container file and all the files inside it might be deleted.

If you choose to quarantine infected documents, you must open those documents in the Quarantine to process the infected documents. You must have the appropriate Role assignments to view quarantined documents.

See "About releasing documents from the Quarantine" on page 219.

See "Assigning Quarantine roles" on page 216.

Configuring scheduled scans

You can create new scheduled scans or modify existing ones. When you no longer need a scheduled scan, you can delete it from the scheduled scan list.

After you create a scheduled scan, you must configure the following scan settings:

- Basics: Provides a description of the scan, the option to enable the scan, and a list of servers that are included in the scan
- Schedule: Contains the scheduled date and time for the scheduled scan

- What to Scan: Contains settings for which databases and directories to scan, which types of attachments to scan, whether to perform content filtering when scanning, whether to scan native MIME message bodies, and the dates and time to perform incremental scans
- Actions: Specifies how to dispose of infected documents found during the scan

To create or modify a scheduled scan

1. In the Settings view, double-click a server group.
2. In the Group document, on the Scan tab, on the Scheduled Scans tab, do one of the following:
   - Double-click an existing scan to modify it.
   - On the Action bar, click **New Scheduled Scan** to set up a new scheduled scan.

To configure scheduled scan basic settings

1. In the Scheduled Scan document, on the Basics tab, under Description, type a meaningful description of the scan so that you can easily identify it in the list of scheduled scans.
2. To enable the scheduled scan that you are configuring, check **Enable this scan**.

   This option is enabled by default.
3. Under Servers, This scan is valid for, select one of the following:
   - All servers in this group: Scans every server in the selected server group

     This option is enabled by default.
   - The following servers: Scans only the servers that you specify

     Select the servers from the drop-down list. Separate multiple entries with commas.
4. On the Action bar, click **Save**.

To configure schedule settings for scheduled scans

1. In the Scheduled Scan document, on the Schedule tab, under Days of the week to run, check the days of the week that you want the scheduled scan to run.

   All of the days are selected by default.
2. Under Times and/or time ranges, type a single time for the scan to start or time ranges for the scan to start and stop.

   The default settings are 4:00 A.M. - 6:00 A.M.

3 To immediately perform a scan after virus definition files are updated, check **Also run this scan after a successful LiveUpdate**.

4 On the Action bar, click **Save**.

To configure what to scan settings for scheduled scans

1 In the Scheduled Scan document, on the What to scan tab, under Databases, select one of the following:

- All databases in the default directory: Scans every database in the Domino\Data directory (default location) for each server in the server group
  This option is enabled by default.
- The following databases and directories: Scans only the databases and directories that you specify
  Type the databases and directories to scan. Separate multiple entries with semicolons (;).

2 To scan subdirectories, check **Include subdirectories**.
Enabling this option scans the descending subdirectories of the default data directory or the directories that you specified.
This option is enabled by default.

3 To exclude specific databases or directories from the scan, under Exclusions, check **Exclude specified databases and directories from scan**.
You must first select these databases and directories on the Configuration > Inclusions/Exclusions tab.
See “Specifying what to scan” on page 84.
This option is enabled by default.

4 Under Attachments, select one of the following:

- Scan all attachments regardless of extension: Scans all attachments
  This option provides the greatest protection against virus attacks and is enabled by default.
- Scan attachments with specified file extensions: Scans only those attachments with file name extensions that are listed in the Specified file extensions option on the Configuration > Inclusions/Exclusions tab

5 To scan for content filtering rule violations, under Content Filtering, check **Scan for Content Filtering rule violations**.
Scanning for content filtering violations is not safe for most databases. Only apply content filtering rules to databases that need to be scanned for a specific type of content filtering rule violation.

6. To scan native MIME message bodies, under Scan Native MIME message bodies, click **On.**

   When this option is enabled, the message body of the infected document is replaced with the text that is specified on the Configuration > Native MIME tab.

   See "Customizing the native MIME message" on page 86.

7. To prevent rescanning of documents, under Incremental Scan, check **Scan only documents modified since last scheduled scan** <last scheduled scan date and time>.

   Click Reset incremental scan date to reset the date to scan all attachments on the next scheduled scan date.

8. On the Action bar, click **Save**.

To configure scheduled scan action settings

1. In the Scheduled Scan document, on the Actions tab, under When a virus is detected, select one of the following:

Log only	Logs the detection but leaves the virus untreated.
Delete the infected attachment	Strips the infected attachment, making it unrecoverable.
Quarantine the document	Holds the infected document in the Quarantine for administrator review.
Repair the infected attachment	Automatically eliminates the virus and repairs any damage. When Symantec Mail Security for Domino cannot repair the document, the selected If unable to repair option applies. This option is enabled by default.

2. Under If unable to repair, select one of the following:
   - Log only
   - Delete the infected attachment
   - Quarantine the document
     This option is enabled by default.

3. On the Action bar, click **Save**.

To delete a scheduled scan

1. In the Group document, on the Scan tab, on the Scheduled Scans tab, in the list of scheduled scans, double-click the scheduled scan that you want to delete.
2. In the Scheduled Scan document, on the Action bar, click **Delete**.
3. In the confirmation dialog box, click **Yes**.
4. On the Action bar, click **Save**.

Configuring LiveUpdate

This chapter includes the following topics:

About LiveUpdate

Symantec Mail Security for Domino relies on up-to-date information to detect and eliminate viruses. One of the most common reasons that you might have a virus problem is that your protection files are not current. Symantec regularly supplies updated virus definition files, which contain the necessary information about all newly discovered viruses.

When you have more than one Symantec product installed on your Lotus Domino server, you need only perform one LiveUpdate session. The virus definitions are shared by the other Symantec products.

See "About shared virus definition files" on page 182.

When LiveUpdate runs, it determines how to connect automatically. You can force LiveUpdate to connect with a specific method. For example, you might have an Internet proxy.

See "Configuring LiveUpdate on a proxy server" on page 183.

LiveUpdate requires an Internet connection. With LiveUpdate, Symantec Mail Security for Domino connects automatically to a Symantec Web site to determine if your virus definitions need updating. If so, it downloads the proper files and installs them in the proper locations. A LiveUpdate connection can be made even when your organization uses a firewall.

See "Using LiveUpdate with a firewall" on page 184.

See "Updating virus protection" on page 185.

You must have a valid content license to use LiveUpdate. A content license is a grant by Symantec Corporation for you to update Symantec corporate software with the latest associated content, such as new virus definitions. When you do not have a content license or your license expires, your product does not receive the most current virus definitions, and your servers are vulnerable to threats.

See "Checking the status of your content license" on page 189.

If you intend to replicate virus definitions across multiple servers, you must create a Definitions database. When Symantec Mail Security for Domino performs a LiveUpdate, the most current virus definitions set is stored in the Definitions database. You can create your own virus definitions set, modify which definitions set to use for scanning, and manage the size of the Definitions database.

See "Managing the Definitions database" on page 190.

Note: Updates to the premium antispam service are handled through the Symantec Premium AntiSpam service and not through LiveUpdate.

See "Before you install and enable the premium antispam service" on page 153.

About shared virus definition files

Symantec Mail Security for Domino can share virus definition files when it runs on the same computer as any of the following Symantec antivirus products:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security

When LiveUpdate is performed from one of these programs, it automatically updates the virus definition files that are used by all of the installed Symantec products.

If you intend to replicate virus definition files using the Symantec Mail Security for Domino Definitions database (savdefs.nsf), you must perform LiveUpdate using Symantec Mail Security for Domino.

Configuring LiveUpdate on a proxy server

Some organizations use proxy servers to control connections to the Internet. To use LiveUpdate, you might need to specify the address and port of the proxy server as well as a user name and password. LiveUpdate can use an HTTP, FTP, or ISP proxy server.

When Internet Explorer is running on the Lotus Domino server and is already configured to use a proxy server, no further configuration is necessary. If needed, you can modify the proxy server configuration settings through LiveUpdate.

To configure FTP settings for LiveUpdate

1. On the Lotus Domino server, on the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for Domino** > **LiveUpdate**.
2. In the LiveUpdate dialog box, click **Configure**.
3. On the FTP tab, click **I want to customize my FTP settings for LiveUpdate**.
   When this setting is checked, the Use a proxy server for FTP connections option appears and is checked by default.
4. In the Address box, type the IP address of the FTP proxy server.
5. In the port box, type the port number.
   Typically, the port number for FTP is 21.
6. Click **OK**.

To configure HTTP settings for LiveUpdate

1. On the Lotus Domino server, on the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for Domino** > **LiveUpdate**.
2. In the LiveUpdate dialog box, click **Configure**.
3. On the HTTP tab, click **I want to customize my HTTP settings for LiveUpdate**.
   When this setting is checked, the Use a proxy server for HTTP connections option appears and is checked by default.
4. In the Address box, type the IP address of the HTTP proxy server.
5. In the port box, type the port number.
   Typically, the port number for HTTP is 80.

6 When a user name and password are required to access the HTTP proxy server, under HTTP Authentication, click **I need authorization to connect through my firewall or proxy server**, and then type the user name and password.

7 Click **OK**.

To use an ISP dial-up connection for LiveUpdate

1 On the Lotus Domino server, on the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for Domino** > **LiveUpdate**.

2 In the LiveUpdate dialog box, click **Configure**.

3 On the ISP tab, click **Customized settings for LiveUpdate**.

4 Under Use this Dial-up Networking connection, do one of the following:

- In the drop-down list, select the appropriate connection.
- If the connection that you want to use is not found in the drop-down list, click **Add**, and then follow the Location Information Wizard instructions to add a connection.

5 Type your ISP user name and password.

6 Click **OK**.

Using LiveUpdate with a firewall

You can use LiveUpdate with a firewall regardless of whether the firewall supports user accounts. You can also use LiveUpdate when your organization uses an internal LiveUpdate server.

To use LiveUpdate with a firewall that supports user accounts

◆ Configure a firewall rule to permit the LiveUpdate connection for the user account of the computer that runs LiveUpdate.

If your firewall has validation rules that are independent of user accounts, LiveUpdate does not work directly. You must install a LiveUpdate server between the firewall and the border router (sometimes referred to as the demilitarized zone or DMZ). Configure your clients to connect with the LiveUpdate server that you installed. Configure the LiveUpdate server that you installed to connect exclusively with the Symantec LiveUpdate server.

To use LiveUpdate with a firewall that does not support user accounts

- If the firewall requires a user name and password, create an FTP proxy server that requires the same user name and password and configure LiveUpdate to use the FTP proxy server.

  LiveUpdate can then pass the same user name and password to both the proxy server and the firewall.

To use LiveUpdate with an internal LiveUpdate server

1. When a firewall rule cannot be configured to permit the LiveUpdate connection, use LiveUpdate Administrator (LUAdmin) to create an internal LiveUpdate server.
2. Manually download virus definitions updates from the Symantec Security Response Web site and apply them to the internal LiveUpdate server.

   For more information, see the LiveUpdate Administrator documentation on the installation CD in the following location: DOCS\LUA\Luadmin.pdf.

Updating virus protection

You can automatically update virus protection using LiveUpdate. LiveUpdate can be configured to run on a scheduled basis, or you can run it on-demand.

See “Updating virus protection with LiveUpdate” on page 185.

You can also update virus definition files without using LiveUpdate. To update virus definition files without LiveUpdate, you need a Web browser.

See “Updating virus protection without LiveUpdate” on page 188.

Updating virus protection with LiveUpdate

Symantec Mail Security for Domino lets you perform LiveUpdate on-demand or automatically on a regular schedule. You can run LiveUpdate on-demand from the Lotus Notes client or from the Domino server console. When you run LiveUpdate on-demand, Symantec Mail Security for Domino uses the connection and download settings that you configured in the Settings database.

You can also configure other LiveUpdate options, such as whether to save virus definitions in the Definitions database, how often to reattempt connections with LiveUpdate if a connection fails, and whom to notify when the license is about to expire or when new definitions arrive. During a virus outbreak, you might want to perform a LiveUpdate session immediately to receive the most current virus definitions.

Scheduling LiveUpdate

You can customize LiveUpdate by configuring the following options:

- Basics: Enable LiveUpdate, indicate whether to save virus definition file to the Definitions database, indicate on which servers the virus definitions apply, and select the day and time to run LiveUpdate sessions.
- Connection: Specify how often to attempt to reconnect if the connection with LiveUpdate fails.
- Notifications: Specify whom to notify for LiveUpdate-related events.

To set LiveUpdate basic options

1. In the Settings view, double-click a server group.
2. In the Group document, on the LiveUpdate tab, on the Basics tab, check **Enable LiveUpdate**.
   This option is enabled by default.
3. To replicate the virus definitions database to other Domino servers, check **Save downloaded virus definitions in the SMSDOM Definitions database**.
   The Definitions database is only required if you plan to replicate virus definitions to other servers. When you select this option, Symantec Mail Security for Domino automatically creates a Definitions database if one does not exist.
   Leave this option unchecked when you have Symantec Mail Security for Domino installed on a single Domino server or you do not plan to replicate the Definitions database.
4. Select one of the following:
   - All servers in this group: LiveUpdate downloads virus definition files to all of the servers in the selected server group.
     This option is enabled by default.
   - The following server: If you choose to replicate virus definitions, then you must select an individual server to run LiveUpdate; otherwise, you may experience save conflicts.
     Select the appropriate server. Ensure that Save downloaded virus definitions in the SMSDOM Definitions database is checked.
5. Under Time of day to run, type the time of day or a range in which to run LiveUpdate.
   If you are configuring LiveUpdate on a high-traffic network, select an off-peak time. The default setting is 3:00 A.M.

6 Under Run LiveUpdate, select the frequency in which to run LiveUpdate.

Generally, weekly updates are sufficient. In a critical installation, run LiveUpdate daily.

The default setting is daily.

7 On the Action bar, click **Save**.

To set LiveUpdate connection options

1 In the Group document, on the LiveUpdate tab, on the Connection tab, under If unable to connect to LiveUpdate server, specify the retry frequency when a connection cannot be made to a LiveUpdate server.

The default setting is to make 3 attempts and to retry each attempt every 20 minutes.

2 On the Action bar, click **Save**.

To set LiveUpdate notification options

1 In the Group document, on the LiveUpdate tab, on the Notifications tab, under When to notify, select any of the following:

When New Definitions Arrive	Symantec Mail Security for Domino has performed a LiveUpdate and new virus definitions were downloaded.
When Product Updates Arrive	Symantec Mail Security for Domino has performed a LiveUpdate and product updates were downloaded and installed.
When Errors Occur	A LiveUpdate was not performed. Possible reasons include a lost connection with the LiveUpdate server or errors in downloading virus definition files or product updates.
When Up-to-Date	LiveUpdate has confirmed that virus definitions and product updates are all up-to-date.
When definitions are older than [14] days	The active virus definitions set is older than the number of days that are specified. The default setting is 14 days.
When license enters warning period or is expired notify me every [14] days	The content license and product license are in the warning period or have expired. The default setting is 14 days.

2 Under Specified users to notify, select who should receive the email notifications.

3 On the Action bar, click **Save**.

Performing LiveUpdate on-demand

You can immediately update virus definitions using the Lotus Notes client or the Domino server.

To perform LiveUpdate on-demand using the Lotus Notes client

1. In the Settings view, double-click a server group.
2. In the Group options, on the LiveUpdate tab, on the Action bar, click **Run LiveUpdate Now**.
3. In the LiveUpdate Status document, on the Action bar, click **Check LiveUpdate Status**.

   A status message appears when LiveUpdate completes the updates.

   See “LiveUpdate status errors” on page 55.

To perform LiveUpdate on-demand using the Domino server

1. On the Domino server, on the Windows taskbar, click **Start** > **Programs** > **Symantec Mail Security for Domino** > **LiveUpdate**.
2. Follow the on-screen instructions to update virus definitions.

Updating virus protection without LiveUpdate

Symantec provides the latest virus definition files for download on the Symantec Web site (http://www.symantec.com) through Intelligent Updater.

The name of the Intelligent Updater file, which changes with each update, uses the following format:

```
yyyymmdd-vvv-Pbb.exe
```

```
  yyyyYear
  mm  Month
  dd  Day
  vvv Version
  P   Processor (I=Intel, A=Alpha)
  bb  Platform (16=16-bit, 32=32-bit)
```

For example, 20040204-003-I32.exe is the February 4, build version three, Intel 32-bit update for Windows 9x/NT/2000.

Note: Use the Windows NT version of Intelligent Updater for Symantec Mail Security for Domino.

To update virus protection without LiveUpdate

1. In a Web browser, type the following address:
   www.symantec.com
2. On the Symantec home page, click the **Downloads** link.
3. On the downloads Web page, click the **Virus Definitions Updates** link.
4. On the Security Response Web page, click the **Download Virus Definitions (Intelligent Updater Only)** link.
5. In the list of Symantec products, click **Symantec Mail Security for Domino**.
6. Click **Download Updates**.
7. Click the program file to begin the download.
   Save the definitions update program to any directory on the server.
8. Run the definitions update program.
   The update program reads the Windows NT registry and installs the necessary files in the proper locations.
9. When the update is complete, delete the definitions update program.

Checking the status of your content license

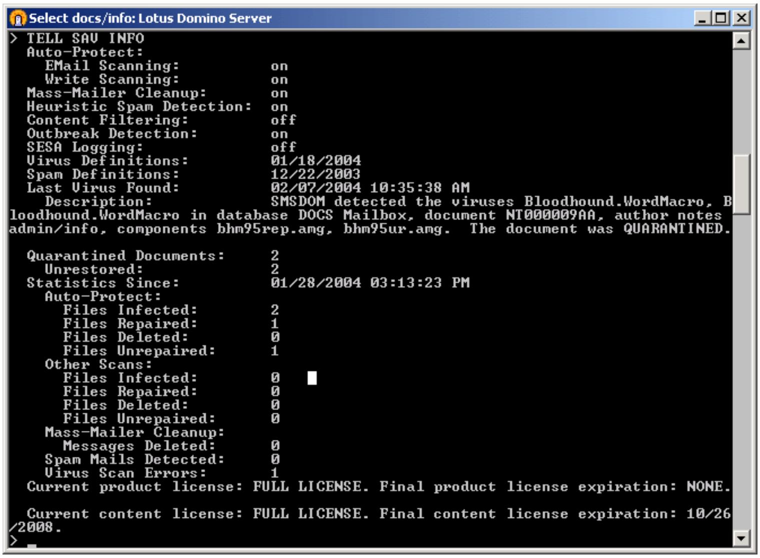
A content license is required to update Symantec corporate software with the latest associated content, such as new virus definitions, through LiveUpdate. A valid content licenses ensures that servers remain protected with the latest virus definitions.

See “About licensing” on page 61.

To check the status of your content license

- Do one of the following:
  - In the Log database, in the left pane, click **Server Messages**.
  - In the Group document, on the Action bar, click **Show Server Status**.
  - Open the Domino console, and at the command prompt, type the following:

    TELL SAV INFO



```
> TELL SAV INFO
  Auto-Protect:
    EMail Scanning:            on
    Write Scanning:            on
  Mass-Mailer Cleanup:         on
  Heuristic Spam Detection:    on
  Content Filtering:           off
  Outbreak Detection:          on
  SESA Logging:                off
  Virus Definitions:           01/18/2004
  Spam Definitions:            12/22/2003
  Last Virus Found:            02/07/2004 10:35:38 AM
    Description:               SMSDOM detected the viruses Bloodhound.WordMacro, B
loodhound.WordMacro in database DOCS Mailbox, document NT000009AA, author notes
admin/info, components bhm95rep.amg, bhm95ur.amg.  The document was QUARANTINED.

  Quarantined Documents:      2
    Unrestored:               2
  Statistics Since:           01/28/2004 03:13:23 PM
    Auto-Protect:
      Files Infected:         2
      Files Repaired:         1
      Files Deleted:          0
      Files Unrepaired:       1
    Other Scans:
      Files Infected:         0
      Files Repaired:         0
      Files Deleted:          0
      Files Unrepaired:       0
    Mass-Mailer Cleanup:
      Messages Deleted:       0
    Spam Mails Detected:      0
    Virus Scan Errors:        1
  Current product license: FULL LICENSE. Final product license expiration: NONE.

  Current content license: FULL LICENSE. Final content license expiration: 10/26
/2008.
>
```

The status that is displayed either states that the content license is valid or that it has expired.

Managing the Definitions database

The Definitions database stores LiveUpdate downloads, which consist of virus definition files. Because the database can be replicated to other Domino servers that run Symantec Mail Security for Domino, only a single LiveUpdate is needed to maintain current protection on all servers.

See “Managing multiple servers” on page 74.

If you do not intend to replicate the Definitions database, this database is not necessary for Symantec Mail Security for Domino operations.

The Definitions database hub stores the active definitions set, in addition to the most recent definitions sets. (A definitions set consists of one or more virus definition files.)

If you choose to replicate virus definitions, and you have created a virus Definitions database, you can manage this database as follows:

- Create a new virus definitions set.
- Select the definitions set to use for scanning.
- Enable the Definitions purge agent to delete older definitions sets.

You can access the Definitions database through the Lotus Notes client or through a Web client.

See “Accessing Symantec Mail Security for Domino” on page 44.

Creating a new virus definitions set

LiveUpdate automatically places virus definition files in the Program Files\Common Files\Symantec Shared\VirusDefs directory, which is used by all Symantec products.

However, you can create your own virus definitions set that consists of the virus definition files that you select.

To create a new virus definitions set

1. On the Lotus Notes client, open the Definitions database.
2. In the Definitions view, on the Action bar, click **New**.
3. In the Definitions document, in the Virus Definitions Date field, modify the date for the new virus definitions set.
   The default setting is the current date.
4. Place your cursor in the Virus Definitions field.
5. On the Lotus Notes file menu, click **File** > **Attach**.
6. In the Create Attachment(s) dialog box, select the virus definition files that you want to add to your new definitions set, and then click **Create**.
   Virus definition files are typically stored in the following location:
   \Program Files\Common Files\Symantec
   Shared\VirusDefs\<numbered_folder>\
7. On the Action bar, click **Save**.
   Symantec Mail Security for Domino automatically calculates the size of the definition set.

Selecting the active definitions set

Each time Symantec Mail Security for Domino performs a LiveUpdate, the virus definitions set that is downloaded is added to the Virus Definitions view and is automatically selected as the active definitions set. However, you can select another definitions set for scanning.

The definitions set that you choose remains active until the next LiveUpdate runs. The next definitions set that is downloaded by LiveUpdate becomes the active definitions set.

To select the active definitions set

1. In the Definitions database view, select the definitions set that you want to use for scanning.
2. On the Action bar, click **Set as Active Definitions**.
   A green check mark appears to the left of the definitions set.

Enabling the Definitions purge agent

LiveUpdate is most effective when you configure it to run automatically at set intervals. Depending on how often you run LiveUpdate, the number of virus definitions sets can quickly accumulate.

See “Updating virus protection” on page 185.

To prevent the Definitions database from growing too large, Symantec Mail Security for Domino can routinely purge virus definitions sets. By default, Symantec Mail Security for Domino keeps the active set of definitions plus the five most recent virus definitions sets. All others are purged.

To enable the Definitions purge agent, you must have rights to run unrestricted agents in the Server Document for the Domino Directory (Public Address Book) that belongs to the server. If you do not have the appropriate rights, you will receive an error message when you attempt to enable the purge agent.

See “Granting rights to run unrestricted agents” on page 47.

To enable the Definitions purge agent

1. On the Lotus Notes client, open the Definitions database using a Notes ID that has the appropriate rights to disable or enable the Definitions purge agent.
2. On the Action bar, click **Set Purge Options**.
3. Type the number of most recent definitions sets to save, including the most current.
   The default setting is 5.

4 In the Purge Options dialog box, click **Set Server to Execute Agent**.

5 In the Choose Server To Run On dialog box, select the server on which the agent should run, and then click **OK**.

6 In the Purge Options dialog box, click **Enable Purge Agent**.

If you receive an error message that indicates that you do not have execution access privileges, contact your administrator to grant you the appropriate purge agent rights.

See “Granting rights to run unrestricted agents” on page 47.

7 Click **OK**.

Using the Symantec Mail Security for Domino Log

This chapter includes the following topics:

About logging

The Symantec Mail Security for Domino Log stores server messages, product information, reports of virus incidents, content filtering rule violations, spam detections, scan summaries, predefined statistical reports, and custom queries.

Server messages and incidents are reported with the following severities:

- Information (blue): No violation occurred with the event.
- Server Warning (purple): No violation occurred with the event, but the server might be experiencing other problems, such as a possible virus outbreak or a disabled or disconnected SESA Agent.
- Warning (green): A violation occurred with the event, but the violation is not deemed critical.
- Critical (red): A violation occurred with the event and it remains.

Note: When Symantec Mail Security for Domino detects a virus in an email message that originated from the iNotes Web Access mail client, it logs the virus incident twice in the Symantec Mail Security for Domino Log database. It processes the virus detection as two separate incidents because when a user sends an email message using iNotes Web Access, the Lotus Domino Web server task writes the message to both the user's mail database and the Mail.box. Consequently, Symantec Mail Security for Domino detects a virus in both databases.

The Lotus Domino Web server task writes the iNotes Web Access email message to both databases, even if the user has set Lotus Notes Preferences not to save sent email messages in the user's mail database.

You can access the Log database through the Lotus Notes client or through a Web client.

See "Accessing Symantec Mail Security for Domino" on page 44.

The incident and information messages that are sent to the Symantec Mail Security for Domino Log are accessed through views. The Log views categorize information to facilitate reviewing and analyzing information. For example, if you only want to see information about viruses that were detected, select the Virus Incidents view. If you only want to see how many violations have occurred based on a specific content filtering rule, select the Statistics/Content Filtering/Violations/All view.

See "Understanding the Log views" on page 197.

Symantec Mail Security for Domino provides several options for managing the Log database. You can view details about incidents and information messages, export incidents to Microsoft Excel, and manage the Log size.

See "Managing the Log" on page 198.

Symantec Mail Security for Domino lets you create custom queries that you can run as needed or on a scheduled basis. You can choose which information to include in the query, such as which type of scan detected the incident, the name of the virus or content filtering rule that triggered the incident, and how Symantec Mail Security for Domino disposed of the document.

See "Customizing queries" on page 203.

Understanding the Log views

You can see the Log data in several views on the Lotus Notes or Web client. Symantec Mail Security for Domino lets you view virus, content filtering, and spam detection data separately.

Table 11-1 lists the Symantec Mail Security for Domino Log views.

Table 11-1 Symantec Mail Security for Domino Log views

Log View	Description
Server Messages	Logs server-related events and displays them by date, type, and message. By default, the Server Messages view sorts by date, but you can sort data by other columns.
Product Information	Logs the Symantec Mail Security for Domino product versions, the servers on which the product is installed, and the version of the most recent virus definitions.
Scan Reports	Logs summaries of scheduled and scan now scans and displays them by date, type, infected (documents), cleaned (documents), and quarantined (documents). By default, the Scan Reports view sorts by date, but you can sort data by other columns.
Incidents	Logs virus detections, spam detections, scan error violations, and content filtering rule violations, and displays them separately or together. Incidents are reported by document, not by database. Symantec Mail Security for Domino uses them to calculate statistics. By default, the Incidents view sorts by date, but you can sort data by other columns. The Incidents views are as follows: ■ All Incidents ■ Virus Incidents ■ Spam Detection Incidents ■ Content Filtering Incidents You can export selected incidents to a Microsoft Excel spreadsheet. See "Exporting incidents to Microsoft Excel" on page 200.

Table 11-1 Symantec Mail Security for Domino Log views

Log View	Description
Statistics	Displays predefined statistical reports of Log data. When you select Virus, Spam Detection, or Content Filtering within the Statistics view, you view data as follows: ■ Organizational/Author ■ Organization/Server ■ Scan Type ■ Viruses (virus statistics only) ■ Spam Score (spam detection statistics only) Spam or suspected spam email messages that are deleted by the premium antispam service are not included in the count. ■ Violations (content filtering statistics only You can select yearly or monthly to add additional sort columns to the view. You can sort data by any column.
Reporting	Displays queries and completed reports that you create. See “Customizing queries” on page 203.

Managing the Log

You can manage the Log in any of the following ways:

- View message and incident documents: Open documents, which provide details about server messages, product information, scan reports, and violation incidents.
  See “Viewing message and incident documents” on page 199.
- Export incidents to Microsoft Excel: Export items from the Incidents view to a Microsoft Excel spreadsheet.
  See “Exporting incidents to Microsoft Excel” on page 200.
- Delete items from the database: Delete messages and incidents from the Log database on-demand.
  See “Deleting items from the Log” on page 201.
- Purge items from the Log: Enable the purge agent to regularly purge items from the Log database.
  See “Enabling the Log purge agent” on page 202.

Viewing message and incident documents

When an incident or a message is logged, a document that contains details about the incident or message is created in the appropriate Log view. (The Statistics and Reporting views do not contain incident or message documents.)

The information that is contained in the document varies depending on whether the item is a server message, product information, a scan report, or an incident.

Table 11-2 lists the information that is contained within a document by view type.

Table 11-2 Message and incident document information

Log view	Description of document information
Server Messages	The Server Message document contains the following information: ■ Server: Server on which the incident occurred. ■ Date: Date and time that the incident occurred or the message was logged. ■ Type: Type of server message (information, server warning, warning, critical). ■ Message: Server message. ■ Link: Link to the incident that triggered the server message (appears only for virus infection, content filtering, or spam incidents).
Product Information	The Symantec Mail Security for Domino Version Information document contains the following information: ■ Server: Server on which Symantec Mail Security for Domino is installed. ■ Virus Definitions version: Active virus definitions set used for scanning. ■ Symantec Mail Security for Domino version: Product version number.

Table 11-2 Message and incident document information

Log view	Description of document information
Scan Reports	The Scan Report document contains the following information: ■ Server: Server on which the scan was performed. ■ Date: Date and time that the scan was performed. ■ Database: Names of the databases that were scanned. ■ Documents scanned: Number of documents that were scanned within a database. ■ Documents violated: Number of documents that contain scan violations. When a document violation is detected, the scan report document also includes information about the document ID, UNID, author, date and time that the document was modified, recipients, the alert notification, and the document disposition.
All Incidents, Virus Incidents, Spam Detection Incidents, Content Filtering Incidents	The Incident document contains detailed information about the incident, such as on which server the incident occurred, the final disposition of the document, and the type of scan that detected the incident.

To view message and incident documents

1. On the Lotus Notes client, open the Log database.
2. In the Log view, on the left pane, select the category that you want to view.
3. In the right pane, select the item for which you want to view a detailed report.
4. To open the document, do one of the following:
   - Double-click the item.
   - On the Action bar, click **Open**.

Exporting incidents to Microsoft Excel

Symantec Mail Security for Domino lets you export incidents that are stored in the Log to a Microsoft Excel spreadsheet. You can select one or more incidents to export.

The option to export incidents to Microsoft Excel is available only in the Lotus Notes client.

To export incidents to Microsoft Excel

1. In the Log, in the left pane, select the Incidents view that contains the incidents that you want to export.
2. In the right pane, to the left of the incident data, select one or more incidents to export.
   A black check mark appears next to the selected items. To unselect an item, click the column again.
3. On the Action bar, click **Export to Excel**.
4. In the Export to Excel dialog box, type the path and file name of the new Microsoft Excel file.
5. Click **OK**.
   This creates a Microsoft Excel spreadsheet that contains the incidents that you selected. The spreadsheet is organized by the columns in the selected Incidents view.

Deleting items from the Log

You can enable the Log purge agent to regularly delete items from the Log. You can also delete an item on-demand to clear the Log view.

See “Enabling the Log purge agent” on page 202.

To delete items from the Log

1. In the Log, in the left pane, select the view that contains the information that you want to delete.
2. In the right pane, click the column to the left of the incident or message that you want to delete.
   A black check mark appears next to the selected items. To unselect an item, click the column again.
3. On the Action bar, click **Delete**.
   A black X appears to the left of the item, which indicates that it is selected for deletion. To unselect the document, click it, and then on the Action bar, click **Delete**.
4. Press **F9** to refresh the view.
5. In the confirmation dialog box, click **Yes**.

Enabling the Log purge agent

To prevent the Log database from growing too large, Symantec Mail Security for Domino can routinely purge documents from the Log views.

A purge agent runs every night at 1:00 A.M., when enabled. By default, virus incidents are purged after 365 days. Other Log entries are purged after 30 days.

If you log a large volume of items, you should modify the purge agent settings to purge documents more often.

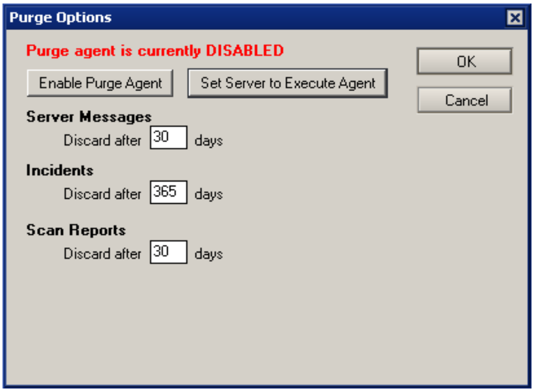
To enable the Log purge agent, you must have rights to run unrestricted agents in the Server Document for the Domino Directory (Public Address Book) that belongs to the server. If you do not have the appropriate rights, you will receive an error message when you attempt to enable the purge agent.

See “Granting rights to run unrestricted agents” on page 47.

To enable the Log purge agent

1 Open the Log database using a Notes ID that has the appropriate rights to disable or enable the Log purge agent.

2 On the Action bar, click **Set Purge Options**.



Purge Options

Purge agent is currently DISABLED

Server Messages
Discard after 30 days

Incidents
Discard after 365 days

Scan Reports
Discard after 30 days

3 In the Purge Options dialog box, do any of the following:

- Under Server Messages, type the number of days to wait to purge server messages.
  The default setting is 30.
- Under Incidents, type the number of days to wait to purge all virus incidents.
  The default setting is 365.
- Under Scan Reports, type the number of days to wait to purge all scan reports.
  The default setting is 30.

After Symantec Mail Security for Domino purges the items, it waits again for the specified number of days before it purges the next batch of items.

4 Click **Set Server to Execute Agent**.

5 In the Choose Server To Run On dialog box, select the server, and then click **OK**.

6 In the Purge Options dialog box, click **Enable Purge Agent**.
If you receive an error message that indicates that you do not have execution access privileges, contact your administrator to grant you the appropriate purge agent rights.
See "Granting rights to run unrestricted agents" on page 47.

7 To exit the dialog box, click **OK**.

Customizing queries

Symantec Mail Security for Domino lets you create custom queries to run on-demand or by schedule. You can design report queries with as much detail and control as needed. To design a query, you specify the conditions of the scan, antispam filtering, or content filtering rule.

For example, you can create a query to collect information about scheduled scans that were performed on a particular server in which Symantec Mail Security for Domino was able to repair a document when a virus was found.

See "Configuring queries" on page 204.

After you create a custom query, you can run it on-demand or on a scheduled basis. After you configure a scheduled query, you must enable it with the Scheduled Report agent. When you no longer need a query or completed report, you can delete it from the Reporting view.

See "Working with queries" on page 209.

See "Enabling the scheduled reports agent" on page 211.

Before you run a query, ensure that the following requirements are met:

- In the Access Control List for the Log database, the Anonymous account must have Read Public Documents and Write Public documents rights.
- The Domino HTTP process must be running and set to TCP port 80.

Configuring queries

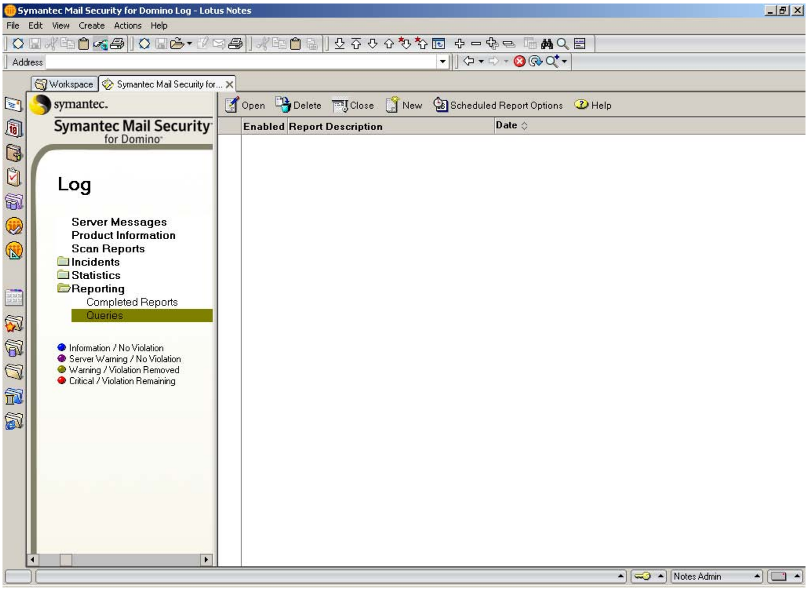
You can configure a query to run once during a time period that you specify, or you can run it repeatedly on a schedule that you create. You can also create and save queries to run on-demand.

After you run a query in Symantec Mail Security for Domino, the completed report appears in the Completed Reports view of the Log.

To configure a query, create a new query or modify an existing one, set basic options for the query, provide specific query information, and define the output criteria.

To create or edit a query

1. In the Log view, in the left pane, click **Reporting**.
2. Under Reporting, click **Queries**.



3 Do one of the following:

- To create a new report, on the Action bar, click **New**.
- To modify an existing query, select an existing query, and then on the Action bar, click **Open**.

To set basic options

1 In the Custom Query document, on the Basics tab, under Report Description, type a description or title for the query.

This description appears in the Reporting, Completed Reports, and Queries views.

2 Under Report Type, select one of the following:

Manual	Specifies a one-time-only query to run in a time range that you specify under Manual Reporting Range. This option is enabled by default.
Scheduled	Specifies that the query be run on a schedule that you specify under Scheduling.

3 To specify the period of time that the query is to gather information, under Manual Reporting Range, do the following:

- Type a beginning and end date, or click the calendar to select a date.
- Type a beginning and end time, or select a time in quarter-hour increments from the list.

  Use the DownArrow to scroll, and click the check mark to close the view and insert your selection.

4 To specify the interval in which to run the query, under Scheduling, check **Enable Scheduled Report**, and then select one of the following:

Daily	This option runs the query every day at 3:00 A.M.
Weekly	After you set and save the Run Interval to Weekly, the query runs at 3:00 A.M. It runs every seven days thereafter at 3:00 A.M. For example, if you set the configuration on Monday at 10:00 A.M., the query will run the next morning at 3:00 A.M. The query will run again the following Tuesday morning at 3:00 A.M., and each Tuesday morning at 3:00 A.M. thereafter, until the configuration is changed or the agent is disabled.

Monthly	After you set and save the Run Interval to Monthly, the query runs at 3:00 A.M. It runs every 30 days thereafter at 3:00 A.M. For example, if you set the configuration on Monday at 10:00 A.M., the query will run the next morning at 3:00 A.M. The query will run again in another 30 days at 3:00 A.M., and every 30 days at 3:00 A.M. thereafter, until the configuration is changed or the agent is disabled. This option is enabled by default.
Quarterly	After you set and save the Run Interval to Quarterly, the query runs at 3:00 A.M. It runs every 120 days thereafter at 3:00 A.M. For example, if you set the configuration on Monday at 10:00 A.M., the query will run the next morning at 3:00 A.M. The query will run again in another 120 days at 3:00 A.M., and every 120 days at 3:00 A.M. thereafter, until the configuration is changed or the agent is disabled.

5 On the Action bar, click **Save**.

To set query information options

1 In the Custom Query document, on the Query Information tab, under Author, select the author (source) of the violation.

The selections are populated from Symantec Mail Security for Domino incidents reports. The default setting is Any Author.

2 Under Server, select the server from which the violation originated.

The selections are populated from the Domino Directory.

3 To specify the type of scan to query for, Under Scan Type, select any of the following:

On Demand	Queries for violations found in scan now scans
Scheduled	Queries for violations found in scheduled scans
Real Time Mail	Queries for violations found in auto-protect scans of email messages
Real Time Writes	Queries for violations found in auto-protect scans of database writes

All options are enabled by default.

4 To specify the type of violation to query for, Under Violation Type, select any of the following:

Virus
This option queries for viruses found in Lotus Notes documents or email message attachments. Available selections are populated from the cumulative total in the Incidents view. After you select the Virus option, in the box below Violation Type, select the virus infection type that you want to query for, or leave it at Any. The list is populated with virus infection types that the Log has captured.

Spam
This option queries for email messages that are identified by the standard or premium antispam engine as spam email.

Content
This option queries for violations in document contents. The violation must match the conditions that are specified on the Content Filtering > Rule tab, where the specified attribute is Body.

All options are enabled by default.

5 To specify documents that Symantec Mail Security for Domino handled in a specific way when it detected a violation, Under Action Taken, select any of the following:

Ignored document
This option queries for only those documents for which Symantec Mail Security for Domino does not act.

Copied document
This option queries for only those documents for which Symantec Mail Security for Domino creates a backup copy after it detects a violation.

Cleaned document
This option queries for only those documents that Symantec Mail Security for Domino repairs.

Removed attachment/ document
This option queries for only those documents or attachments that Symantec Mail Security for Domino deletes.

Quarantined document
This option queries for only those documents or attachments that Symantec Mail Security for Domino quarantines.

Delivered document to recipient's spam folder
This option queries for only those documents that were detected by the premium antispam engine as spam or suspected spam and were delivered to the spam folder of the email recipient using the foldering agent.

See "Automatically routing messages to a spam folder" on page 231.

Modified message — This option queries for only those documents that were detected as spam or suspected spam and in which the X-header or subject line were modified.

All options are enabled by default.

6 To select all of the options under Scan Type, Violation Type, and Action Taken, click **Select All**.

7 On the Action bar, click **Save**.

Note: Symantec Mail Security for Domino cannot query for scan error violations.

To set output options

1 To select the level of detail for the query, in the Custom Query document, on the Output tab, under Report Type, select one of the following:

Summary Totals Only — Shows the total number of incidents. For each incident, shows the date and time that the violation was detected, the document author, the server on which the violation occurred, the action Symantec Mail Security for Domino took with the document, and the violation name (for example, virus name, content filtering rule, or spam score or verdict).

Detailed Report — For each incident, shows the date and time that the violation was detected, the document author, the server on which the violation occurred, the action Symantec Mail Security for Domino took with the document, and the violation name (for example, virus name, content filtering rule, or spam score or verdict).

Detailed Report with Summary Totals — Shows the total number of incidents. For each incident, shows the date and time that the violation was detected, the document author, the server on which the violation occurred, the action Symantec Mail Security for Domino took with the document, and the violation name (for example, virus name, content filtering rule, or spam score or verdict).

This option is enabled by default.

2 Under Output Format, select one of the following:

Plain Text (CSV format)	When the selected Output Destination is the Log Report, this option writes the query to a rich text field in the Log database. When the destination is a file, this option writes the query to a comma-delimited file (.csv) file. This format can be imported into Microsoft Excel. This option is enabled by default.
XML	This option writes the query to an XML file. You can use this format with many other programs.
HTML	This option writes the query to an HTML file.

3 Under Output Destination, select any of the following:

Log Report	This option writes the query to the Symantec Mail Security for Domino Log database, regardless of the Output Format that you choose. This option is enabled by default.
Write Report to File	This option writes the query to a file, which is saved to the location that you select. Click the button next to the file name box to select the file. The format of the file is determined by the Output Format. This option is enabled by default.
Send Report In Email To	Sends the query through email to the person that you select. Click the drop-down list to open the Lotus Notes Select Addresses dialog box.

4 On the Action bar, click **Save**.

5 To return to the Queries view, on the Action bar, click **Close**.

Working with queries

You can create manual queries to run on-demand, or you can schedule queries to run at the times that you specify. For easier identification in the Queries view, you can specify in the description that the query is scheduled or manual.

When you create a scheduled query and enable it, a check mark appears next to it in the Queries view. Before the query can run, you must also enable the schedule reports agent, which enables all of the scheduled queries to run.

See “Enabling the scheduled reports agent” on page 211.

Manual queries are always turned off because you run them on-demand only. Manual queries do not have a check mark under the Enabled column in the Queries view to distinguish them from the scheduled queries.

To run a manual query and view it

1. In the Log view, in the left pane, click **Reporting**.
2. Under Reporting, click **Queries**.
3. In the Queries view, in the right pane, double-click the manual query to open it.
4. In the Custom Query document, on the Action bar, click **Run Report Now**.
5. To return to the Queries view, on the Action bar, click **Close**.
6. In the left pane, under Reporting, click **Completed Reports**.
7. Double-click the report to view it.

To delete queries in the Queries view

1. In the Queries view, in the right pane, click the column to the left of the queries that you want to delete.
   A black check mark appears next to the selected items. To unselect an item for deletion, click the column again.
2. On the Action bar, click **Delete**.
   A black X appears to the left of the item, which indicates that it is selected for deletion. To unselect an item, click it, and then on the Action bar, click **Delete**.
3. Press **F9** to refresh the view.
4. In the confirmation dialog box, click **Yes**.

To delete reports in the Completed Reports view

1. In the Completed Reports view, in the right pane, click the column to the left of the completed reports that you want to delete.
   A black check mark appears next to the selected items. To unselect an item for deletion, click the column again.
2. On the Action bar, click **Delete**.
   A black X appears to the left of the item, which indicates that it is selected for deletion. To unselect an item, click it, and then on the Action bar, click **Delete**.
3. Press **F9** to refresh the view.
4. In the confirmation dialog box, click **Yes**.

Enabling the scheduled reports agent

You must enable the scheduled reports agent to run scheduled queries. This agent runs all of the scheduled queries that are enabled (signified by a check mark under the Enabled column in the Queries view) once a day. Query results are posted in the Completed Reports view.

You must individually enable each scheduled query that you want to run.

See “Working with queries” on page 209.

Manual queries do not need to be individually enabled or disabled.

The first time that you enable the scheduled reports agent, Symantec Mail Security for Domino prompts you for the server on which to run the agent. Symantec Mail Security for Domino replicates the scheduled reports agent.

To enable the scheduled reports agent, you must have rights to run unrestricted agents in the Server Document for the Domino Directory (Public Address Book) that belongs to the server. If you do not have the appropriate rights, you will receive an error message when you attempt to enable the scheduled reports agent.

See “Granting rights to run unrestricted agents” on page 47.

To enable the scheduled reports agent

1. In the Queries view, on the Action bar, click **Scheduled Reports Options**.
2. In the Scheduled Reports Agent dialog box, click **Enable Scheduled Reports Agent**.
3. Select the server on which to run the agent.
   If you receive an error message that indicates that you do not have execution access privileges, contact your system administrator to grant you the appropriate agent rights.
   See “Granting rights to run unrestricted agents” on page 47.
4. Click **OK**.

Chapter 12

Managing the Quarantine

This chapter includes the following topics:

About the Quarantine

Symantec Mail Security for Domino can isolate scanned documents that have triggered violations. It can also back up infected documents before you delete or attempt to repair them. Quarantined and backup documents are stored in the Symantec Mail Security for Domino Quarantine database.

When an email message is quarantined, Symantec Mail Security for Domino places the entire email message and any attachments in the Quarantine database, regardless of which part of the email message is infected or has offending content. It does not forward any part of the email message. Symantec Mail Security for Domino can also quarantine infected Lotus Notes database documents.

See "Managing quarantined documents" on page 214.

As a data safety precaution, administrators can configure Symantec Mail Security for Domino to store a backup copy of any document or email message that contains content filtering rule violations or infected attachments.

See "Managing backup documents" on page 228.

See "Creating backup documents" on page 86.

To prevent the Quarantine database from growing too large, Symantec Mail Security for Domino can routinely purge documents from the Quarantine.

See "Purging the Quarantine" on page 229.

The separation of the Quarantine from the Log lets Symantec Mail Security for Domino replicate the Log database and gather statistical information for multiple servers without simultaneously having to handle the additional overhead and disk space that quarantined and backup documents require.

Symantec Mail Security for Domino displays quarantined documents separately from backup documents. You can further sort these views by recipient, SMTP originator, content filtering rule violations, and virus infections.

Incidents are reported with the following severities:

- Information (blue): No violation occurred with the event.
- Warning (green): A violation occurred with the event, but the violation is not deemed critical.
- Critical (red): A violation occurred with the event, and it remains.

You can access the Quarantine database through the Lotus Notes client or through a Web client.

See "Accessing Symantec Mail Security for Domino" on page 44.

Managing quarantined documents

You can access information about quarantined documents through Quarantine views. Views categorize the quarantined documents to make it easier to view and manage the Quarantine.

See "About Quarantined Documents views" on page 215.

You must be assigned the appropriate roles to access information and to perform specific functions within the Quarantine. For example, to release a content filtering rule violation document from the Quarantine, you must have the CFReleaser role. You assign user roles to the Symantec Mail Security for Domino Quarantine by using the Access Control List.

See "Assigning Quarantine roles" on page 216.

With the appropriate Quarantine role assignments, you can perform specific tasks within the Quarantine, such as releasing documents from the Quarantine, viewing the content that triggered a content filtering rule violation, or deleting an infected document attachment.

See "Actions to manage quarantined documents" on page 218.

You can release documents that are held in the Quarantine if you have the appropriate Quarantine roles. For virus infected documents, you must first delete the infected attachment before releasing the document. Documents held in the Quarantine for virus infections are rescanned before they are sent to their destinations.

Symantec Mail Security for Domino treats documents that are unscannable, contain encrypted container files, or exceed container limits as scan error violations. Scan error violation documents are not scanned when they are released from the Quarantine.

For documents and email messages that trigger a content filtering rule violation, if you have the appropriate Quarantine roles, you can view the body of the message that triggered the violation. Documents held in the Quarantine for content filtering rule violations are not rescanned when they are released from the Quarantine.

See “About releasing documents from the Quarantine” on page 219.

When Symantec Mail Security for Domino scans a document, it is possible that the document might trigger multiple types of violations. For example, a document might contain a virus, a content filtering rule violation, and an encrypted container file.

When a document contains multiple violation types, Symantec Mail Security for Domino quarantines the document based on the most severe violation that it detects. For example, if a document contains a virus infection and a content filtering rule violation, it is quarantined by Symantec Mail Security for Domino as an infected document.

See “About multiple violation types” on page 220.

You manage the Quarantine by performing specific tasks, such as viewing and adding comments to a Quarantine Document, adding, saving, or deleting attachments, releasing documents from the Quarantine, or deleting documents from the Quarantine view.

See “Managing quarantined infected documents” on page 220.

About Quarantined Documents views

Most of the Quarantined Documents views show when the document was quarantined, which database was affected, who authored the document, and which virus or content filtering rule was involved. The views also show whether the document was released or restored to its original database.

Table 12-1 lists the Quarantined Documents views.

Table 12-1 Quarantined Documents views

View	Description
All Quarantined Documents	All quarantined documents
By Recipient	Email messages or documents, sorted by recipient
By SMTPOriginator	Email messages that were received from the Internet, sorted by email message origin
Content Filtering Violations	Email messages or documents that contain at least one content filtering rule violation
Virus Infections	Email messages or documents that contain at least one virus infection

You can open a Quarantined Document in any view. For content filtering rule violations, you can also open an additional document that contains the content that triggered the violation, which can help you determine whether to release the document. It can also help you fine-tune your content filtering rules. For example, after you view the content of a quarantined message, you might decide that the content filtering rule that found the violation is too restrictive. You might want to reduce the applicable threshold value for that rule.

See "Creating a content filtering rule" on page 118.

To view or take action on any Quarantined Document, you must be assigned to the appropriate Quarantine role.

Assigning Quarantine roles

The Quarantine database uses roles to restrict access to documents that are in the Quarantine. You assign roles to Symantec Mail Security for Domino users through the Access Control List. These roles determine who can see the documents in the Quarantine and who can perform actions on them. For example, many of your users might be assigned roles that let them view all documents that contain content filtering rule violations or virus infections but restrict them from viewing the offending content of the content filtering rule violations.

Table 12-2 lists the Quarantine roles that you can assign.

Table 12-2 Quarantine roles

Role	Description
CFViewer	Lets the user see backup and quarantined documents that contain content filtering rule violations, and lets the user add, save, or delete attachments in those documents
CFContentViewer	Gives the user the same access as the CFViewer, plus the rights to see the content that triggered the violation
CFReleaser	Gives the user the same access as the CFViewer, plus the rights to release quarantined documents that contain content filtering rule violations
VirusViewer	Lets the user see backup and quarantined documents that contain the infected or scan error violations, and lets the user add, save, or delete attachments
VirusReleaser	Gives the user the same access as the VirusViewer, plus the rights to release quarantined documents that contain virus infections (provided the infected attachment is deleted from the document) and scan error violations

Only users who have the appropriate role assignments can view, manage, or release quarantined documents.

You must manually add the appropriate users or groups to the Access Control List of the Quarantine database and assign them the appropriate Quarantine roles. You should assign all Quarantine roles to the LocalDomainServers group and the current server, or add them to the groups that you are using. Otherwise, the database does not replicate properly.

To assign Quarantine roles

1. Log on to the account that you plan to use to administer Symantec Mail Security for Domino.
2. In the Lotus Notes workspace, right-click the Quarantine database, and then click **Database** > **Access Control**.
3. In the Access Control List dialog box, ensure that the appropriate users or groups to manage the Quarantine are added to the Access Control List as Managers with Delete Documents rights.

4 In the Roles box, select one or more roles for each user or group to manage the Quarantine.
See "Assigning Quarantine roles" on page 216.

5 On the Access Control List dialog box, click **OK**.

Actions to manage quarantined documents

Table 12-3 lists the actions that you can take to manage quarantined documents. These items appear as icons on the Action bar in the Quarantine Document. Only those actions that are appropriate to your role appear on the Action bar.

Table 12-3 Quarantined Document actions

Action	Description
Save Attachments	Saves a copy of the attachment or attachments in a location that you choose. After you save a copy, you should run another scan to repair it (perhaps using updated virus definitions), or forward it to Symantec Security Response for repair. After it is repaired, you can add the attachment to the quarantined document again and release it to its recipient. If the attachment contains a content filtering rule violation, you can save it in a location where someone can review it before deciding what further action to take. You must have the CFViewer or VirusViewer roles to save attachments.
Add Attachment	Adds the file that you select as an attachment to the quarantined document. Before you release a document from the Quarantine, you can add a newly repaired compressed file, replace an infected file with a known good copy, or add a procedural file with instructions to scan a workstation. You must have the CFViewer or VirusViewer roles to add attachments.
Delete Attachments	Deletes the attachments. Symantec Mail Security for Domino prompts you to confirm the action before deleting each one. When you delete attachments, the quarantined document remains in the Quarantine view without the attachments. You must have the CFViewer or VirusViewer roles to delete attachments.

Table 12-3 Quarantined Document actions

Action	Description
Release (virus infections only)	Releases the document from the Quarantine. When you release a document, Symantec Mail Security for Domino changes the Restored field from No to Yes. The quarantined document remains in the Quarantine until Symantec Mail Security for Domino purges it or you delete it from the view. You must have the VirusReleaser role to release infected documents.
View Content Violation (content filtering rule violations only)	Opens an expanded view of the content filtering rule violation document to show the content that triggered the violation. You must have the CFContentViewer role to see the content that triggered the violation.
Unscanned Release (scan error violations and content filtering rule violations only)	Releases scan error violation or content filtering rule violation documents, but flags them so that the scan engine does not process them again for violations. If the document is subsequently routed to another server or is modified, Symantec Mail Security for Domino scans it again as a new document. When you release a document, Symantec Mail Security for Domino changes the Restored field from No to Yes. You must have the CFReleaser role to release documents that contain content filtering violations only. You must have the VirusReleaser role to release documents that contain any scan error violations. See "About multiple violation types" on page 220.

About releasing documents from the Quarantine

One of the actions that you can perform in the Quarantine is to release a document to its destination. When you release a content filtering rule violation document, it is not rescanned before it goes to its destination.

You must delete infected attachments before you can release an infected document from the Quarantine. The document is rescanned before it reaches its destination to ensure it is free from viruses.

Documents that contain encrypted containers, exceed container limits, or are unscannable are treated as scan error violations. Because a scan error violation is unscannable, when you release it from the Quarantine, the document is not rescanned before it is sent to its destination. Use caution when you release scan error violation documents from the Quarantine because they may still be a threat for malicious attacks. As a best practice, ensure that the client is adequately protected.

For example, an email message is quarantined because it contains an encrypted container file. It is released from the Quarantine by the administrator and sent to its destination. The recipient of the email message uses a valid password to open the encrypted file. If the encrypted file contains a virus, the client is vulnerable to the virus infection if the client does not have adequate virus protection.

About multiple violation types

When documents are scanned, they might trigger more than one type of violation. For example, a document might be infected with a virus, and it might contain a content filtering rule violation.

When a document is infected and contains one or more content filtering rule violations, the document is quarantined as an infected document. When you delete the infected attachment and release the document from the Quarantine, the document is scanned again. After it is rescanned, if Symantec Mail Security for Domino is configured to quarantine content filtering rule violations, the document is quarantined again as a content filtering rule violation.

When a document contains a scan error violation and one or more content filtering rule violations, it is quarantined as an infected document. However, when you release the document from the Quarantine, it is not rescanned. Because the document is not rescanned, even when Symantec Mail Security for Domino is configured to quarantine content filtering rule violations, the document is not returned to the Quarantine as a content filtering rule violation.

Managing quarantined infected documents

You manage infected documents from the All Quarantined Documents, By Recipient, By SMTPOriginator, or Virus Infections views. Ensure that you have at least VirusViewer roles before you open the Quarantine, or you will not see any quarantined documents.

See “Assigning Quarantine roles” on page 216.

Before you can release an infected document from the Quarantine database, you must ensure that it no longer contains infected attachments. You can make an infected attachment safe by deleting it, replacing it, or repairing it. You can release documents only when you are assigned the VirusReleaser role.

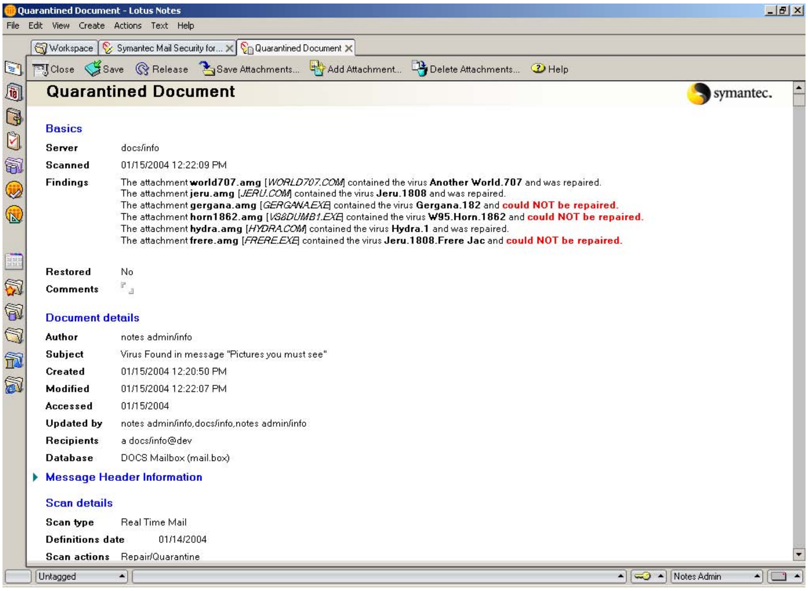
You can manage quarantined infected documents in any of the following ways:

- View a Quarantined Document: The Quarantined Document contains basic information about a specific violation, which includes document details, message header information, and scan details.
- Create a comment in the Quarantined Document: Add your customized comments in the Quarantined Document.
- Modify (save, delete, or add) attachments: Save attachments to a specified location, delete infected attachments, or add your own attachments to a document before you release it.
- Release the document from the Quarantine: Release a document from Quarantine after the infection is deleted.
- Delete an infected document from the database: Delete the quarantined document and all of its attachments from the Quarantine database.

To view a Quarantined Document

1. On the Lotus Notes client, open the Quarantine database.
2. In the left pane, under Quarantined Documents, select one of the following views:
   - All Quarantined Documents
   - By Recipient
   - By SMTPOriginator
   - Virus Infections

3 In the right pane, double-click a document.



Quarantined Document

Basics

Server	docs/info
Scanned	01/15/2004 12:22:09 PM
Findings	The attachment **world707.amg** [*WORLD707.COM*] contained the virus **Another World.707** and was repaired. The attachment **jeru.amg** [*JERU.COM*] contained the virus **Jeru.1808** and was repaired. The attachment **gergana.amg** [*GERGANA.EXE*] contained the virus **Gergana.182** and **could NOT be repaired.** The attachment **horn1862.amg** [*VS8DUMB1.EXE*] contained the virus **W95.Horn.1862** and **could NOT be repaired.** The attachment **hydra.amg** [*HYDRA.COM*] contained the virus **Hydra.1** and was repaired. The attachment **frere.amg** [*FRERE.EXE*] contained the virus **Jeru.1808.Frere Jac** and **could NOT be repaired.**
Restored	No
Comments	

Document details

Author	notes admin/info
Subject	Virus Found in message "Pictures you must see"
Created	01/15/2004 12:20:50 PM
Modified	01/15/2004 12:22:07 PM
Accessed	01/15/2004
Updated by	notes admin/info,docs/info,notes admin/info
Recipients	a docs/info@dev
Database	DOCS Mailbox (mail.box)

Message Header Information

Scan details

Scan type	Real Time Mail
Definitions date	01/14/2004
Scan actions	Repair/Quarantine

This document contains the Action bar icons that are available to users with the VirusReleaser role.

To create a comment in the Quarantined Document

- In the Quarantined Document, in the Comments field, type your comments.

To modify attachments

- In the Quarantined Document, on the Action bar, select one of the following:
  - Save Attachments: For each attachment, you are prompted to save the file to a location that you select.
  - Add Attachment: You are prompted to type the path of the file that you want to add.

    After adding the attachment, press **F9** to refresh the document.
  - Delete Attachments: For each attachment, you are prompted to confirm the action before the attachment is deleted.

    After deleting the attachment, press **F9** to refresh the document.

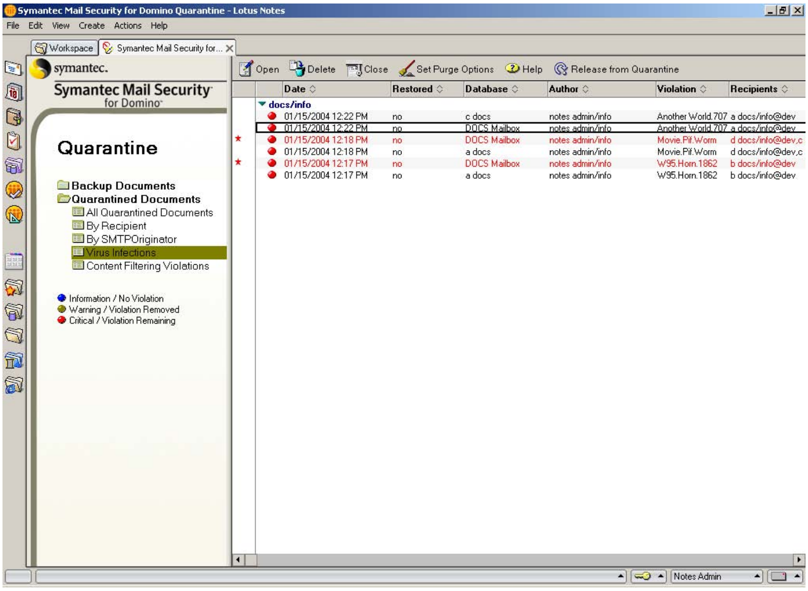
To release a document from Quarantine after viewing it

1. In the Quarantined Document, on the Action bar, click **Release**.
2. In the Confirm release of quarantined documents dialog box, click **Yes**.
3. In the confirmation dialog box, click **Yes**.

Released documents remain in the Quarantine until Symantec Mail Security for Domino purges them or you delete them.

To release a document from the Quarantine without viewing it

1. In the Quarantine view, in the left pane, under Quarantined Documents, click **Virus Infections**.


Symantec Mail Security for Domino Quarantine - Lotus Notes
File
Edit
View
Create
Actions
Help
Workspace
Symantec Mail Security for...
symantec.
Symantec Mail Security for Domino
Quarantine
Backup Documents
Quarantined Documents
All Quarantined Documents
By Recipient
By SMTPOriginator
Virus Infections
Content Filtering Violations
Information / No Violation
Warning / Violation Removed
Critical / Violation Remaining
Open
Delete
Close
Set Purge Options
Help
Release from Quarantine
Notes Admin

docs/info

	Date	Restored	Database	Author	Violation	Recipients
	01/15/2004 12:22 PM	no	c docs	notes admin/info	Another World.707	a docs/info@dev
	01/15/2004 12:22 PM	no	DOCS Mailbox	notes admin/info	Another World.707	a docs/info@dev
★	01/15/2004 12:18 PM	no	DOCS Mailbox	notes admin/info	Movie.Pif.Worm	d docs/info@dev,c
	01/15/2004 12:18 PM	no	a docs	notes admin/info	Movie.Pif.Worm	d docs/info@dev,c
★	01/15/2004 12:17 PM	no	DOCS Mailbox	notes admin/info	W95.Hom.1862	b docs/info@dev
	01/15/2004 12:17 PM	no	a docs	notes admin/info	W95.Hom.1862	b docs/info@dev

2. In the right pane, select the documents that you want to release from the Quarantine.
3. On the Action bar, click **Release from Quarantine**.
   Documents will be rescanned and then delivered to their destinations.
4. In the confirmation dialog box, click **Yes**.

Released documents remain in the Quarantine until Symantec Mail Security for Domino purges them or you delete them.

To delete a quarantined document from the database

1. In the Quarantine, in the left pane, under Quarantined Documents, select one of the following views:
   - All Quarantined Documents
   - By Recipient
   - By SMTPOriginator
   - Virus Infections
2. In the right pane, select the document that you want to delete.
3. On the Action bar, click **Delete.**
   A black X appears to the left of the document, which indicates that it is selected for deletion. To unselect the document, click it, and then on the Action bar, click **Delete**.
4. Press **F9** to refresh the view.
5. In the confirmation dialog box, click **Yes**.

Managing quarantined content filtering rule violation documents

You can manage content filtering rule violations from the All Quarantined Documents, By Recipients, By SMTPOriginator, and Content Filtering Violations views. Ensure that you have at least CFViewer roles before you open the Quarantine, or you will not see any quarantined documents.

See “Assigning Quarantine roles” on page 216.

When the quarantined document has a content filtering rule violation, you can release it or any attachment without changing or replacing the document or attachment. When you are assigned a CFContentViewer role, you see the text that triggered the content filtering rule violation, which can help you decide whether to release the document. It can also help you fine-tune the content filtering rule or rules that caused the document to be quarantined. Documents that contain content rule violations are not rescanned when they are released from the Quarantine.

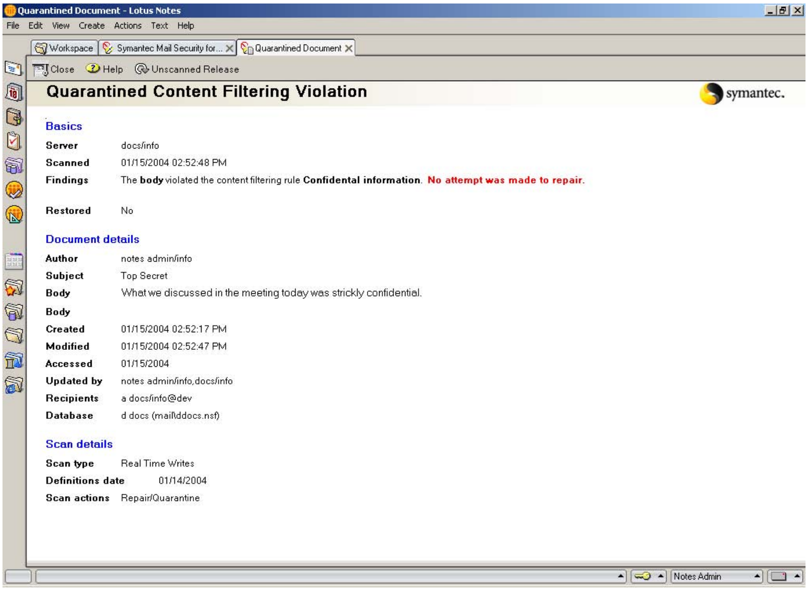
You can manage quarantined content filtering rule violation documents in any of the following ways:

- View a Quarantined Document: The Quarantined Document contains basic information about a specific violation, which includes document details and scan details. If you are assigned the CFContentViewer role, you can view the body of the document that contains the violation.
- Create a comment in the Quarantined Document: Add your customized comments in the Quarantined Document.

- Modify (save, delete, or add) attachments: Save attachments to a specified location, delete attachments, or add your own attachment to the file before you release the document.
- Release a document from the Quarantine: Release a document from Quarantine. Content filtering rule violation documents are not rescanned when they are released from the Quarantine.
- Delete a content filtering rule violation document from the database: Delete the quarantined document and all of its attachments from the Quarantine database.

To view the Quarantined Document

1. In the Quarantine, in the left pane, under Quarantined Documents, select one of the following views:
   - All Quarantined Documents
   - By Recipient
   - By SMTPOriginator
   - Content Filtering Violations
2. In the right pane, double-click a document to view the Quarantined Document.
3. On the Action bar, click **View Content Violations**.


Quarantined Document - Lotus Notes
File Edit View Create Actions Text Help
Workspace
Symantec Mail Security for...
Quarantined Document
Close
Help
Unscanned Release
symantec.
Notes Admin

Quarantined Content Filtering Violation

Basics

Server	docs/info
Scanned	01/15/2004 02:52:48 PM
Findings	The **body** violated the content filtering rule **Confidental information**. **No attempt was made to repair.**
Restored	No

Document details

Author	notes admin/info
Subject	Top Secret
Body	What we discussed in the meeting today was strickly confidential.
Body	
Created	01/15/2004 02:52:17 PM
Modified	01/15/2004 02:52:47 PM
Accessed	01/15/2004
Updated by	notes admin/info,docs/info
Recipients	a docs/info@dev
Database	d docs (mail\ddocs.nsf)

Scan details

Scan type	Real Time Writes
Definitions date	01/14/2004
Scan actions	Repair/Quarantine

To create a comment in the Quarantined Document

- In the Quarantined Document, in the Comments field, type your comments.

To modify attachments

- In the Quarantined Document, on the Action bar, select one of the following:
    - Save Attachments: For each attachment, you are prompted to save the file to a location that you select.
    - Add Attachment: You are prompted to type the path of the file that you want to add.

      After adding the attachment, press **F9** to refresh the document.
    - Delete Attachments: For each attachment, you are prompted to confirm the action before it is deleted.

      After deleting the attachment, press **F9** to refresh the document.

To release a document from the Quarantine after viewing it

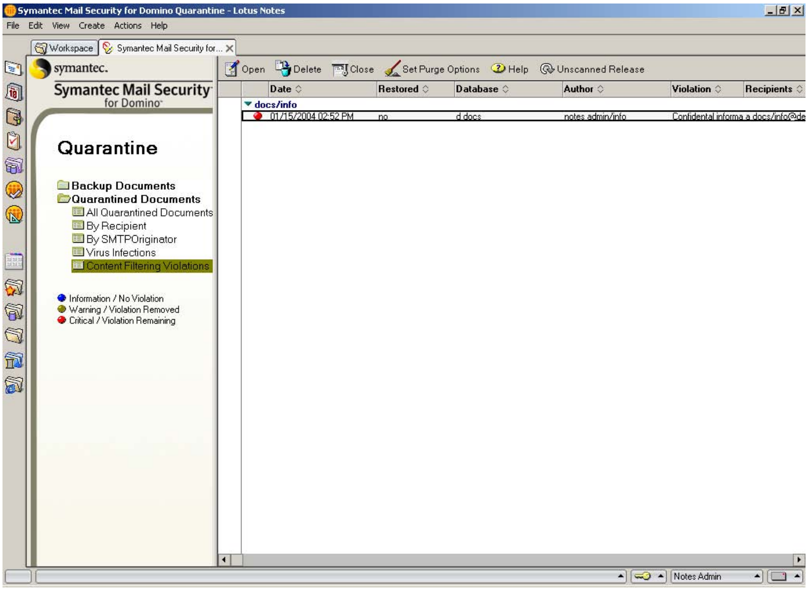
1. In the Quarantined Document, on the Action bar, click **Unscanned Release**.
2. In the confirmation dialog box, click **Yes**.
3. When you are prompted to save your changes, click **Yes**.

   Released documents remain in the Quarantine until Symantec Mail Security for Domino purges them or you delete them.

To release a document from the Quarantine without viewing it

1 In the Quarantine view, in the left pane, under Quarantined Documents, click **Content Filtering Violations**.

2 In the right pane, select the document that you want to release.



● Information / No Violation
● Warning / Violation Removed
● Critical / Violation Remaining

Date	Restored	Database	Author	Violation	Recipients
docs/info					
● 01/15/2004 02:52 PM	no	d docs	notes admin/info	Confidental informa	a docs/info@de

3 On the Action bar, click **Unscanned Release**.

4 In the confirmation dialog box, click **Yes**.
Released documents remain in the Quarantine until Symantec Mail Security for Domino purges them or you delete them.

To delete a content filtering rule violation document from the database

1 In the Quarantine, in the left pane, under Quarantined Documents, select one of the following views:

- All Quarantined Documents
- By Recipient
- By SMTPOriginator
- Content Filtering Violations

2 In the right pane, select the document that you want to delete.

3. On the Action bar, click **Delete**.
   A black X appears to the left of the document, which indicates that it is selected for deletion. To unselect the document, click it, and then on the Action bar, click **Delete**.
4. Press **F9** to refresh the view.
5. In the confirmation dialog box, click **Yes**.

Managing backup documents

You can configure Symantec Mail Security for Domino to make a backup copy of infected documents before it attempts to repair or delete them.

See “Creating backup documents” on page 86.

You can manage backup documents in one of the following views:

All Backup Documents	All backup documents
By Recipient	Backup email messages or documents, sorted by recipient
By SMTPOriginator	Backup email messages or documents that were received over the Internet with violations, sorted by email origin
Virus Infections	Backup email messages or documents with virus infections
Content Filtering Violations	Backup email messages or documents with content filtering rule violations

You can manage backup documents by viewing the Backup Document, saving attachments, and deleting documents. You must have at least the CFViewer role and the VirusViewer role to see backup documents.

To view a Backup Document

1. In the Quarantine, in the left pane, click **Backup Documents**.
2. Under Backup Documents, select one of the following views:
   - All Backup Documents
   - By Recipient
   - By SMTPOriginator
   - Virus Infections
   - Content Filtering Violations
3. In the right pane, double-click a document.

To save attachments

- In the Backup Document, click **Save Attachments**.
  You are prompted to save each attachment separately to a location that you select.

To delete a document

1. In any Backup Document view, in the right pane, select the document that you want to delete.
2. On the Action bar, click **Delete**.
   A black X appears to the left of the document, which indicates that it is selected for deletion. To unselect the document, click it, and then on the Action bar, click **Delete**.
3. Press **F9** to refresh the view.
4. In the confirmation dialog box, click **Yes**.

Purging the Quarantine

A purge agent runs every night at 1:00 A.M., when enabled. By default, Symantec Mail Security for Domino purges entries after 30 days. If you have a large volume of quarantined documents, you can modify the purge agent settings to purge documents more often.

To enable the Quarantine purge agent, you must have rights to run unrestricted agents in the Server Document for the Domino Directory (Public Address Book) that belongs to the server. If you do not have the appropriate rights, you will receive an error message when you attempt to enable the purge agent.

See “Granting rights to run unrestricted agents” on page 47.

To purge the Quarantine

1. Open the Quarantine database using a Notes ID that has the appropriate rights to disable or enable the Quarantine purge agent.
2. On the Action bar, click **Set Purge Options**.
3. In the Purge Options dialog box, under Quarantine Items, do any of the following:
   - Type the number of days to wait to purge virus infections from the Quarantine view.
   - Type the number of days to wait to purge scan error and content filtering rule violations from the Quarantine Documents view.

4 Under Backup Items, do any of the following:

- Type the number of days to wait to purge virus infections from the Backup Documents view.
- Type the number of days to wait to purge scan error and content filtering rule violations from the Backup Documents view.

5 In the Purge Options dialog box, click **Set Server to Execute Agent**.

6 In the Choose Server To Run On dialog box, select the server on which you want to run the agent, and then click **OK**.

7 In the Purge Options dialog box, click **Enable Purge Agent** to enable the agent.
If you receive an error message that indicates that you do not have execution access privileges, contact your administrator to grant you the appropriate purge agent rights.
See "Granting rights to run unrestricted agents" on page 47.

8 Click **OK**.

Appendix A

Automatically routing messages to a spam folder

This chapter includes the following topics:

- About the foldering agent
- Setting up the foldering agent

About the foldering agent

The Symantec Premium AntiSpam foldering agent lets you automatically route unwanted messages to a spam folder. It relieves users and administrators of the burden of using their mail clients to create filters. The foldering agent creates a subfolder and a server-side filter in the mailbox of each user. The agent applies the filter to messages that Symantec Premium AntiSpam identifies as spam email and then routes the spam email into the user's spam folder. The foldering agent also lets users submit missed spam and false positives to their administrators and to the Symantec Brightmail Logistics and Operations Center (BLOC).

See "Disposing of spam messages using premium antispam" on page 163.

How the foldering agent works

Symantec Premium AntiSpam appends an X-header to filtered spam or suspected spam. The foldering agent creates a server-side rule that searches for the X-header. It also creates a spam subfolder in the mailbox of each user. During its hourly maintenance schedule, the agent routes spam messages to the spam folder for each recipient. If the agent detects that the spam folder for a given recipient has been deleted or moved, it recreates the subfolder. The rule runs as a high sequence number (1001), which ensures that it runs after rules with lower sequence numbers and after any client-side rules that users may have created.

The mail server on which you install the foldering agent distributes changes to all other mail servers in your environment as part of the Designer task. This task runs overnight.

The spam folder only appears in the mail folder of a user after one of the following occurs:

- Replication distributes the change to the template on the home mail server
- The nightly Designer process runs on the home mail server
- A user reopens the mail file after installation
  This only applies if the mail file of a user is open when its design is refreshed. The foldering agent takes effect when the design is refreshed, although the folder will not be visible.

For more information on forcing changes, see the Lotus Notes documentation.

Setting up the foldering agent

The foldering agent is an application that is designed to work with the Symantec Premium AntiSpam service. The foldering agent is not installed when you install the premium antispam service. You must install the foldering agent using a separate installation program that is located on the Symantec Mail Security for Domino installation CD.

See “Installing the foldering agent” on page 233.

You configure the foldering agent when you install it. To reconfigure the foldering agent after installation, you must uninstall it, and then reinstall it.

See “Uninstalling the foldering agent” on page 235.

To use the foldering agent, you must first install and enable the premium antispam service.

See “Enabling and disabling the premium antispam service” on page 159.

If you want to run the foldering agent on Lotus Notes 5.0.11, 5.0.12, or 5.0.13, additional configuration is required after you install the agent.

See “After installing the foldering agent on Lotus Notes 5.0.1x” on page 234.

Installing the foldering agent

You must install the foldering agent on each Lotus Domino mail server on your network.

Before you install the foldering agent, ensure that the server and clients meet the system requirements.

See "System requirements" on page 31.

To install the foldering agent

1. On the server on which you want to install the agent, insert the Symantec Mail Security for Domino CD into the CD-ROM drive.
2. Copy the following database from the Symantec Mail Security for Domino CD on to your local server:
   ADMTOOLS\Folder_Agent.nsf
3. In Lotus Notes, on the File menu, click **Database** > **Open**.
4. In the Open Database dialog box, under Server, click **Local**.
5. Under Database, click **Brightmail Domino Agent**.
6. Click **Open**.
7. In the agent installer wizard, in the Welcome document, click **Install Domino Agent**, and then click **Next**.
8. In the License Agreement document, click **I accept the terms of the license agreement**, and then click **Next**.
9. In the Preparing to Install document, read the on-screen instructions to ensure that you have completed all prerequisite steps, and then click **Next**.
10. In the Selecting Options document, select any of the following:
    - Install Spam Folder: Creates a spam folder in Lotus Notes for each user.
    - Install Submissions Capability: Lets users submit false positives or missed spam to the Symantec Brightmail Logistics Operations Center.
11. Click **Next**.
12. In the Configuring Spam Folder Information document, under Spam Folder, type the name of the folder to which spam messages should be routed.
    The default is Spam.

13 Under Spam Expiration, type the number of days in which a spam message remains in the user's spam folder before it is automatically deleted, and then click **Next**.

The expiration period must be between 1 and 365 days. Messages will be automatically deleted from the spam folder after the specified number of days. The default is 30 days.

14 In the Configuring Submissions document, select the types of misclassified mail that users can submit to the Symantec Brightmail Logistics and Operations Center.

15 To receive a copy of each users' misclassified email submissions, under Local Administrator Email for Submissions, do one of the following:

- Click the drop-down list and select an email address
- Type an email address

16 Click **Next**.

17 Type the name of the server on which you want to install the foldering agent.

If your mail template files are replicas (as they are when shipped), you only need to install the foldering agent on one server.

18 Type the name of the mail template that you want to modify.

Repeat this step for each mail template that you want to modify.

19 Click **Install**.

20 Click **Finish**.

See "After installing the foldering agent on Lotus Notes 5.0.1x" on page 234.

21 Configure Symantec Mail Security for Domino to deliver spam email to the spam folder of the recipient.

See "Disposing of spam messages using premium antispam" on page 163.

After installing the foldering agent on Lotus Notes 5.0.1x

If you want to run the foldering agent on Lotus Notes 5.0.11, 5.0.12, or 5.0.13, you must add the following variable to the Notes.ini file on each server in your environment:

```
Amgr_DisableMailLookup=1
```

You should then restart each server.

Note: The Notes.ini file is usually found in the server's root Notes folder.

Distributing Help files to users

The foldering agent lets users submit missed spam and false positives to their administrators and to the Symantec Brightmail Logistics and Operations Center. The foldering agent installer includes a Microsoft Word file (BMIEndUser.doc) that details the submission process.

You can distribute this information to users in one of the following ways:

- Send all users an email message that includes the document as an attachment.
- Add the information from the BMIEndUser.doc to the Help Using document of the mail template so that users have it available at all times.

For more information, see your Lotus Notes documentation.

Uninstalling the foldering agent

You uninstall the foldering agent from the foldering agent database.

To uninstall the foldering agent

1. On the Lotus Notes workspace, double-click **Brightmail Domino Agent**.
2. Click **Uninstall foldering agent**, and then click **Next**.
3. Click **Uninstall**.
   If your mail template files are replicas (as they are when shipped), you only need to uninstall the agent once.
4. Click **Finish**.

Appendix B

Integrating Symantec Mail Security for Domino with SESA

This chapter includes the following topics:

- About SESA
- Interpreting Symantec Mail Security for Domino events in SESA
- Configuring logging to SESA
- Uninstalling SESA

About SESA

In addition to using the Symantec Mail Security for Domino Log, you can also log events to the Symantec Enterprise Security Architecture (SESA). SESA is an underlying software infrastructure and a common user interface framework. It integrates multiple Symantec Enterprise Security products and third-party products to provide a central point of control of security within an organization. It provides a common management framework for SESA-enabled security products, such as Symantec Mail Security for Domino, that protect your IT infrastructure from malicious code, intrusions, and blended threats.

SESA increases your organization's security posture by simplifying the task of monitoring and managing the multitude of security-related events and products that exist in today's corporate environments. SESA includes an event management system that employs data collection services for events that are generated on computers that are managed by Symantec security products. The event categories and classes include antivirus, content filtering, network security, spam, and systems management. The range of events varies depending on the Symantec applications that are installed and managed by SESA.

You can monitor and manage these security-related events through the SESA Console. The SESA Console is the common user interface that provides manageable integration of security technologies (Symantec or otherwise), Symantec Security Services, and Symantec Security Response. You can query, filter, and sort data to reduce the security-related events that you see through the SESA Console, which lets you to focus on threats that require your attention. You can configure alert notifications in response to events, and generate, save, and print tabular and graphical reports of event status, based on filtered views that you create.

SESA is purchased and installed separately. SESA must be installed and working properly before you can configure Symantec Mail Security for Domino to log events to SESA.

For more information, see the SESA documentation.

Interpreting Symantec Mail Security for Domino events in SESA

SESA provides extensive event management capabilities, such as common logging of normalized event data for SESA-enabled security products like Symantec Mail Security for Domino. The event categories and classes include antivirus, content filtering, network security, spam, and systems management. SESA also provides centralized reporting capabilities, including graphical reports. The events that are forwarded to SESA by Symantec Mail Security for Domino take advantage of the existing SESA infrastructure for events.

You can create alert notifications for certain events. Notifications include pagers, SNMP traps, email messages, and operating system Event Logs. You can define the notification recipients, day and time ranges when specific recipients are notified, and custom data to accompany the notification messages.

For more information about interpreting events in SESA and on the event management capabilities of SESA, see the SESA documentation.

Symantec Mail Security for Domino can send the following types of events to SESA:

- Application events
- Security events

Application events that are sent to SESA

Table B-1 lists the application events that Symantec Mail Security for Domino can send to SESA.

Table B-1 Application events that are sent to SESA

Event ID (SES_EVENT_<Unique ID>)	Severity	Event class	Rule Description (Reason sent)
APPLICATION_START	Informational	BASE	Task Initializes
APPLICATION_STOP	Informational	BASE	Task is shutdown
DATA_SCAN_CANCEL	Informational	DATA_SCAN	Scheduled Scan sent to run for a set amount of time and does not finish before that time is over OnDemand Scan stopped from console Task is shutdown before OnDemand or Scheduled Scan can finish
DATA_SCAN_END	Informational	DATA_SCAN	OnDemand or Scheduled Scan completes successfully Task is shut down (for Real-time scan)
DATA_SCAN_PAUSE	Informational	DATA_SCAN	Before Updating Settings Before Updating Definitions
DATA_SCAN_RESUME	Informational	DATA_SCAN	After Updating Settings After Updating Definitions
DATA_SCAN_START	Informational	DATA_SCAN	Initialize time for Real-time An OnDemand or Scheduled Scan starts
VIRUS_DEFINITION_UPDATE	Informational	DEFUPDATE	Definitions are updated

Security events that are sent to SESA

Table B-2 lists the security events that Symantec Mail Security for Domino can send to SESA.

Table B-2 Security events that are sent to SESA

Event ID (SES_EVENT_<Unique ID>)	Severity	Event class	Rule Description (Reason sent)
GENERIC_CONTENT	Warning	DATA_INCIDENT	[Content filtering rule name]
SPAM_CONTENT	Warning	DATA_INCIDENT	For Standard Antispam, Spam score: [ ]% For Premium Antispam, Spam score: [spam] or [suspected spam]
UNSCANNABLE_VIOLATION	Warning	DATA_INCIDENT	Virus scan error
VIRUS	Warning: Deleted/Repaired Minor: Quarantined Major: Infected (Log only)	DATA_VIRUS_INCIDENT	Detect viruses Mass-mailer cleanup

Configuring logging to SESA

The logging of events to SESA is in addition to logging events in the Symantec Mail Security for Domino Log database. Logging to SESA is activated independently of the Symantec Mail Security for Domino Log. If you have purchased SESA, you can send a subset of the events that are logged by Symantec Mail Security for Domino to SESA.

To configure logging to SESA, you must complete the following steps:

Configure SESA to recognize Symantec Mail Security for Domino	For SESA to receive events from Symantec Mail Security for Domino, you must run the SESA Integration Wizard that is specific to Symantec Mail Security for Domino on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying the individual security product (in this case, Symantec Mail Security for Domino) to SESA. See "Configuring SESA to recognize Symantec Mail Security for Domino" on page 241.
Install a local SESA Agent on the computer that is running Symantec Mail Security for Domino	The local SESA Agent handles the communication between Symantec Mail Security for Domino and SESA. See "Installing the local SESA Agent using the Agent Installer" on page 243.
Configure Symantec Mail Security for Domino to send logging events to SESA	You use the administrative interface to configure Symantec Mail Security for Domino to communicate with the local SESA Agent and to log events to SESA. See "Configuring Symantec Mail Security for Domino to log events to SESA" on page 248.

Configuring SESA to recognize Symantec Mail Security for Domino

To configure SESA to receive events from Symantec Mail Security for Domino, run the SESA Integration Wizard on each computer that is running the SESA Manager. The SESA Integration Wizard installs the appropriate integration components for identifying Symantec Mail Security for Domino to SESA. You must run the SESA Integration Wizard for each SESA Manager computer to which you are forwarding events from Symantec Mail Security for Domino.

Before running the SESA Integration Wizard, you must copy the SESA Integration Package (datapackage.sip) from the Symantec Mail Security for Domino CD to your local computer.

Note: Installation of the SESA Integration Package is only supported on Domino DB2 databases.

To configure SESA to recognize Symantec Mail Security for Domino

1. On the computer on which SESA Manager 2.0 is installed, create a folder for the datapackage.sip file, for example:
   C:\Datapackage
2. Insert the Symantec Mail Security for Domino CD into the CD-ROM drive.
3. Copy the following file to the newly created folder:
   ADMTOOLS/SESA_SIPI_for_SMSDOM/datapackage.sip
4. On the computer on which the SESA Manager is installed, insert the SESA CD1 - SESA Manager CD into the CD-ROM drive.
5. At the command prompt, change directories on the CD to the following location:
   \SIPI
6. To start the SESA Integration Wizard, at the command prompt, type:
   ```
   java -jar setup.jar
   ```
7. In the SESA Integration Wizard, click **Next** until you see the SESA Domain Administrator Information window.

8 In the SESA Domain Administrator Information window, type the specific information about the SESA Domain Administrator and the SESA Directory.

SESA Domain Administrator Name	The name of the SESA Directory Domain Administrator account.
SESA Domain Administrator Password	The password for the SESA Directory Domain Administrator account.
IP Address of SESA Directory	The IP address of the computer on which the SESA Directory is installed (may be the same as the SESA Manager IP address if both are installed on the same computer). When you are using authenticated SSL instead of SESA default, anonymous SSL, you must type the host name of the SESA Directory computer. For example, mycomputer.com. For more information about SESA default, anonymous SSL and upgrading to authenticated SSL, see the *Symantec Enterprise Security Architecture Installation Guide*.
SSL Port	The number of the SESA Directory secure port. The default port number is 636.

9 In the SESA Integration Package to Install window, click **Browse** and locate the datapackage.sip file, and then click **OK**.

10 Click **Next.**

11 Follow the on-screen instructions to install the appropriate SESA Integration Package and complete the SESA Integration Wizard.

12 Repeat steps 1 through 11 on each SESA Manager computer to which you are forwarding Symantec Mail Security for Domino events.

Installing the local SESA Agent using the Agent Installer

The local SESA Agent handles the communication between Symantec Mail Security for Domino and SESA and is installed on the same computer that is running Symantec Mail Security for Domino. The local SESA Agent is provided as part of the software distribution package for Symantec Mail Security for Domino. A separate installation package for installing the Agent, sesa_agent_installer.exe, is located in the ADMTOOLS\SESA_Agent_Installer directory on the installation CD for Symantec Mail Security for Domino.

When you have more than one SESA-enabled product installed on a single computer, these products can share a local SESA Agent. However, each product must register with the Agent. Thus, even if an Agent has already been installed on the computer for another SESA-enabled security product, you must run the installer to register Symantec Mail Security for Domino.

The local SESA Agent is preconfigured to listen on IP address 127.0.0.1 and port number 8086. Symantec Mail Security for Domino uses this information to communicate with the Agent. If you must change the IP address or port number for the Agent, you must do so through the SESA Console. (After an Agent is installed, it is controlled through the SESA Console, even though it is running on the same computer that is running the security product.) You must also update, through the Symantec Mail Security for Domino Settings database, the information that Symantec Mail Security for Domino uses to contact the local SESA Agent.

For more information, see the SESA documentation.

See “Configuring Symantec Mail Security for Domino to log events to SESA” on page 248.

Before you install the SESA Agent, install the Java Runtime Environment (JRE) version 1.3.1_02 on the server on which the SESA Agent will be installed. This program is provided on the Symantec Mail Security for Domino installation CD in the following folder: ADMTOOLS\JRE\j2re-1_3_1_02-win.exe.

To install the SESA Agent using the SESA Agent Installer that Symantec Mail Security for Domino provides, run the Installer on all computers on which Symantec Mail Security for Domino is installed.

To install the local SESA Agent using the Agent Installer

1. On the computer on which you have installed Symantec Mail Security for Domino, insert the Symantec Mail Security for Domino installation CD into the CD-ROM drive.
   The installation program launches automatically. If it does not, run cdstart.exe from the installation CD.
2. In the Installation window, click **Install SESA Agent** to begin the installation process.
3. In the Introduction panel, read the on-screen information, and then click **Next**.
4. In the License Agreement panel, indicate that you accept the terms of the Symantec license agreement, and then click **Next**.
   You must accept the terms of the license agreement for the installation to continue.

5 In the Readme panel, read the on-screen information, and then click **Next**.

6 In the Choose Install Folder panel, do one of the following:

- To install the SESA Agent in the default location, click **Next**.
- To install the SESA Agent in another location, click **Choose**, browse to the folder in which you want to install the SESA Agent, click **Select**, and then click **Next**.

7 In the Register Additional Services panel, from the list of products to register with SESA, check **Symantec Mail Security for Domino**, and then click **Next**.

You can register only one product at a time. If you are installing the SESA Agent to work with more than one Symantec product, you must run the installer again for each product.

8 In the Primary SESA Manager Information panel, do the following:

- In the Primary SESA Manager Host/IP name box, type the IP address or host name of the computer on which the primary SESA Manager is running.

  If SESA is configured to use anonymous SSL (the default setting), type the IP address of the primary SESA Manager. If SESA is configured to use authenticated SSL, type the host name of the primary SESA Manager (for example, computer.company.com).
- In the Primary SESA Manager port number box, type the port number on which the SESA Manager listens, and then click **Next**.

  The default port number is 443.

9 In the Secondary SESA Manager Information panel, if you are running a Secondary SESA Manager that is to receive events from Symantec Mail Security for Domino, do the following:

- In the Secondary SESA Manager Host/IP address name box, type the IP address or host name of the computer on which the Secondary SESA Manager is running.
- In the Secondary SESA Manager Port number box, type the port number on which the Secondary SESA Manager listens, and then click **Next**.

  The default port number is 443.

10 In the Agent Domain Information panel, in the Organizational Unit Domain name box, type the organizational unit distinguished name to which the Agent will belong.

If the organizational unit is unknown or not yet configured, this setting can be left blank. Use the following format:

ou=Europe,ou=Locations,dc=SES,o=symc_ses

The domain(s) (dc=) portion of the path should correspond to the domain that is managed by the selected SESA Management Server.

11 In the Agent Start-up Mode panel, select one of the following:

- Start SESA Agent Automatically: The SESA Agent starts automatically whenever the computer is restarted.
- Start SESA Agent Manually: You must manually restart the SESA Agent each time that the computer is restarted.

12 Check **Start the SESA Agent at installation completion** to let the SESA Agent start immediately after the installation finishes, and then click **Next** to continue.

If you leave the box unchecked, you must manually start the SESA Agent after the installation is complete.

13 In the Pre-Installation Summary panel, review the information that you configured in the SESA Agent Installer wizard.

14 When you are finished, on the Install complete panel, click **Done**.

When the installation is complete, the Agent is installed and is listed as SESA AgentStart Service in the Services Control Panel.

Installing the SESA Agent manually by command line

You can install the SESA Agent by command line.

To manually install the SESA Agent, you do the following:

- Prepare to install the SESA Agent.
- Install the SESA Agent by command line.
- Start the SESA AgentStart Service

To prepare to install the SESA Agent

1 On the computer on which Symantec Mail Security for Domino is installed, create a folder for the SESA Agent files, for example:

C:\Agent

2 Insert the SESA CD1 - SESA Manager CD into the CD-ROM drive.

3 Copy the files from the \Agent folder on the CD and paste them in the newly created folder on the Symantec Mail Security for Domino computer.

4 In a text editor, open the Agent.settings file, for example:
C:\Agent\Agent.settings

5 Change the value of the mserverip setting to the IP address of the SESA Manager to which Symantec Mail Security for Domino forwards events.

6 Save and close the Agent.settings file.

To install the SESA Agent by command line

1 On the computer on which Symantec Mail Security for Domino is installed, at the command prompt, change to the folder in which the SESA Agent files reside, for example:
C:\Agent

2 At the command prompt, type the following:

```
java -jar agentinst.jar -a3008
```

3008 is a unique product ID to install the Agent for Symantec Mail Security for Domino. To remove the SESA Agent, you must use the same product ID parameter (for Symantec Mail Security for Domino, 3008).
Optionally, you can append any of the following parameters:

-debug	Writes logging information to the screen
-log	Turns off the installation log and instructs the SESA Agent to write logging information to the Agntinst.log file in the local Temp directory

To start the SESA AgentStart Service

1 On the computer on which you installed the SESA Agent, on the Windows taskbar, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Administrative Tools**.

3 In the Administrative Tools window, double-click **Services**.

4 In the Services dialog box, right-click **SESA AgentStart Service**.

5 Click **Start**.

Configuring Symantec Mail Security for Domino to log events to SESA

After you have installed the local SESA Agent to handle communications between Symantec Mail Security for Domino and SESA, you must configure Symantec Mail Security for Domino to communicate with the Agent by specifying the IP address and port number on which the Agent listens. You must also ensure that logging to SESA is activated. These settings are located on the Symantec Mail Security for Domino Settings database.

To configure Symantec Mail Security for Domino to log events to SESA

1. In the Settings view, double-click a server group.
2. On the Configuration tab, on the Logging tab, under Where to Log, check **Enable SESA logging**.
3. In the SESA agent IP address[:Port Number] box, type the IP address and port on which the local SESA Agent listens.

   The default IP setting is 127.0.0.1 (the loopback interface), which restricts connections to the same computer.

   The port number that you type here must match the port number on which the local SESA Agent listens. The default port is 8086.
4. On the Action bar, click **Save**.

Uninstalling SESA

When Symantec Mail Security for Domino is no longer forwarding messages to SESA, you can uninstall the SESA components.

Uninstalling the SESA Integration Package

You can uninstall the SESA Integration Package from each computer that is running the SESA Manager using the Add or Remove Programs option in the Windows Control Panel.

To uninstall the SESA Integration Package

1. In the Windows Control Panel window, double-click **Add or Remove Programs**.
2. In the Add or Remove Programs window, click **SESA Agent**.
3. Click **Change/Remove**.
4. In the Uninstall SESA Agent panel, click **Uninstall**.

5. In the confirmation dialog box, click **Uninstall the SESA Agent**.
6. Click **Done**.

Uninstalling the local SESA Agent

The local SESA Agent is automatically uninstalled when you uninstall Symantec Mail Security for Domino. When more than one product is using the Agent, the uninstall script removes only the Symantec Mail Security for Domino registration and leaves the Agent in place. When no other security products are using the Agent, the uninstall script uninstalls the Agent as well.

Index